



**NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY**

**Faculty of Computing and Informatics
Department of Informatics**

DEVELOPING A CYBERSECURITY FRAMEWORK FOR THE BANKING SECTOR OF NAMIBIA

Thesis submitted in fulfilment of the requirements for the degree of

Master of Informatics

at the

Namibia University of Science and Technology

Presented by:	Eva-Lisa Tuwilika Nawa
Student Number:	214062414
Supervisor:	Prof Fungai Bhunu Shava
Co-Supervisor:	Dr Mercy Chitauro
Submission Date:	20 August 2021

METADATA

TITLE: Ms

STUDENT NAME: Eva-Lisa Tuwilika Nawa

SUPERVISOR: Prof Fungai Bhunu Shava

CO-SUPERVISOR: Dr Mercy Chitauro

DEPARTMENT: Informatics

QUALIFICATION: Master of Informatics

SPECIALISATION: Cybersecurity

STUDY TITLE: Developing a cybersecurity framework for the banking sector of Namibia

KNOWLEDGE AREA: Cybersecurity

KEYWORDS: Cybersecurity, framework, financial sector

TYPE OF RESEARCH: Applied Research

METHODOLOGY: Interpretivism

STATUS: Final Thesis

SITE: Main Campus Windhoek

DOCUMENT DATE: 20 August 2021

SPONSOR: Deutscher Akademischer Austauschdienst (DAAD)

DECLARATION

I, **Eva-Lisa Tuwilika Nawa**, student number **214062414**, hereby declare that the work contained in this thesis for the Master of Informatics Degree project, entitled:

“Developing a cybersecurity framework for the financial sector of Namibia”, is my own original work and that I have not previously in its entirety or in part submitted it at any university or other higher education institution for the award of a degree.

I further declare that I have fully acknowledged all sources of information I have used for the research in accordance with the Institution rules.

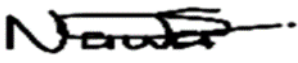
Signature: 

Date: 20 August 2021

RETENTION AND USE OF THESIS

I, **Eva-Lisa Tuwilika Nawa** being a candidate for the degree of Master of **Informatics** accept the requirements for the Namibia University of Science and Technology relating to the retention and use of thesis deposited in the Library and Information Services.

In terms of these conditions, I agree that the original of my thesis deposited in the Library and Information Services will be accessible for purpose of study and research, in accordance with the normal conditions established by the Librarian for the care, loan or reproduction of the thesis.

Signature: 

Date: 20 August 2021

ACKNOWLEDGEMENTS

I would like to express my gratitude to the Almighty God for the unconditional love, protection, wisdom, good health and for the gift of life.

I am especially grateful to my supervisors, Prof Fungai Bhunu Shava and Dr Mercy Chitauro for their guidance, leadership and unconditional support. Prof and Dr, thank you for your determination, trust, timely feedback and patience which brought this study to finality. Thanks for your unwavering faith in me, but, most of all, thank you for being uniquely you. That gentle pressure, yet realistic, made a difference, and it's the reason this journey came to an end.

A great acknowledgement is extended to my parents Mr and Mrs Nawa, for the love and unconditional support throughout my life and studies. I am who I am today because of your love, support, encouragement and good upbringing. I would also like to extend my gratitude to my academic mentor, Dr Jude Osakwe, who truly inspired and encouraged me, and who has always been available when I needed his support. I am indebted to your kindness and selfless support.

I would also like to acknowledge the management of the six Namibian licensed banks and the entire teams for the time they took to participate in the questionnaire and the framework evaluation. Thank you so much ladies and gentlemen, your contribution towards my study is immensely appreciated, I would not have completed this study without your input.

Lastly, my acknowledgement is extended to my sisters, brothers, friends, cousins, and all family relatives as well as everyone that has supported me throughout this study.

Thank you all.

ABSTRACT

The banking sector represents a vast assortment of firms, agencies and institutions with operations ranging from small community banks to massive international corporations. Managing the banking sector in Namibia presents a herculean task to regulators charged with its regulation oversight on cyber risks. The management of cybersecurity takes on greater complexity in considering multinationals with global partners and operations in countries with varying levels of cybersecurity sophistication. With the increase of cyber-attacks worldwide and banking institutions being key targets, the degree of risks from cybersecurity threats that banks are facing has grown rapidly in recent years. The increasing threats place sensitive data and organisational security at risk. This is exacerbated by the absence of a recognised cybersecurity framework that can safeguard the online transactions of financial data between banks and customers in the banking sector. To overcome these problems, a Namibia Banking Cybersecurity Framework (NBCF) to guide banking institutions in safeguarding the online transactions of financial data between banks and customers was developed. A qualitative research approach using the Design Science Research Methodology (DSRM) was adopted to address the research objectives. This research was conducted in the commercial banks of Namibia and involved their staff. In addition to data collected from literature reviews, data were also collected from a sample of 6 out of 10 licenced banks in Namibia using semi-structured interviews. The selection of the banks was done using the purposive sampling method and universally accepted ethical standards were considered. Data were analysed through a technique known as coding. The study identified various elements which are essential for a cybersecurity framework: data protection and privacy, human factors such as soft skills, Principle of Least Privilege (POLP), public knowledge on information security practices, aspect of disaster recovery documentation, and cyber breach simulations. The NBCF framework is proposed as a guideline on how the Namibian banking institutions can securely build cyber resiliency, manage their cyber risks and strategies and also help in implementing an appropriate level of rigor for their cybersecurity programmes. The NBCF framework should therefore guide the adoption of cybersecurity best practices in the Namibian banking sector. In addition, the framework is envisaged to complement the current Namibian government initiatives and the long-term goals of Vision 2030 such as the strategy of attaining

infrastructure development as stated in the Harambee Prosperity Plan which highlights the urgent necessity to invest in cybersecurity. Expert reviews of the proposed framework were conducted and they yielded that the framework is relevant, applicable, usable and understandable in combating cybersecurity issues in the Namibian banking sector.

Keywords: cybersecurity, cybercrimes, banking sector, cybersecurity frameworks

PUBLICATIONS

Nawa, E., Chitauro, M., & Bhunu Shava, F. (2021). *Assessing patterns of cybercrimes associated with online transactions in Namibia banking institutions' cyberspace*. 15th International Multidisciplinary Information Technology and Engineering Conference. (IMITEC2021).

Contents

DECLARATION iii

RETENTION AND USE OF THESIS iii

ACKNOWLEDGEMENTS iv

ABSTRACT v

PUBLICATIONS vii

LIST OF FIGURES xii

LIST OF TABLES xiii

ABBREVIATION AND ACRONYMS IN THIS THESIS xv

CHAPTER ONE: INTRODUCTION 1

 1.1 Background 1

 1.2 Problem Statement 2

 1.2.1 Research Objectives 3

 1.2.2 Research Questions 3

 1.3 Significance of the Study 4

 1.4 Justification of the Study 4

 1.5 Delimitation 5

 1.6 Thesis Outline 5

 1.7 Chapter Summary 6

CHAPTER TWO: LITERATURE REVIEW 7

 2.1 Overview 7

 2.2 An Overview of Cybercrime 7

 2.3 Global Current Cybersecurity Attacks in the Banking Sector 8

 2.4 Impact and Growth of Cybercrime on the Banking Sector 11

 2.5 Internet Use in Namibia 13

2.6 Cybersecurity Policy and Strategy in Namibia.....	13
2.7 Existing Cybersecurity Frameworks, Best Practices and Standards.....	16
2.7.0 Introduction.....	16
2.7.1 National Institute of Standards and Technology (NIST) Cybersecurity Framework ..	17
2.7.2 The CPMI-IOSCO Cybersecurity Framework	20
2.7.3 ISO/IEC 27001:2013 Standards on Information Security Management Systems	21
2.7.4 Center for Internet Security (CIS).....	22
2.7.5 A Framework for the Governance of Information Security in Banking System	24
2.8 Research Gaps in the Existing Frameworks	31
2.9 Chapter Summary	33
CHAPTER THREE: RESEARCH METHODOLOGY	35
3.1 Overview.....	35
3.2 Research Paradigm.....	35
3.3 Research Design.....	37
3.4 Data Collection	38
3.5 Research Population.....	45
3.6 Sample and Sampling Technique.....	46
3.7 Data Analysis for Qualitative Research.....	47
3.8 Data Analysis Plan.....	49
3.8.1 Data Collection and Management.....	50
3.8.2 Organising and Preparing Data	51
3.8.3 Coding and Describing Data	51
3.8.4 Conceptualisation, Classifying, Categorising, Identifying Themes.....	52
3.8.5 Connecting and Interrelating Data	52
3.8.6 Interpretation, Creating Explanatory Accounts, Providing Meaning	52

3.9 Research Methodology Limitations	53
3.10 Assumptions.....	53
3.11 Ethical Considerations	54
3.12 Chapter Summary	54
CHAPTER FOUR: DATA ANALYSIS.....	55
4.1 Overview.....	55
4.2 Analysis of Data.....	55
4.2.1 Data Collection Management	55
4.2.2 Organising and Preparing Data.....	55
4.2.3 Coding and Describing Data.....	62
4.2.4 Conceptualisation, Classifying, Categorising and Identifying Themes.....	73
4.2.5 Connecting and Interrelating Data.....	74
4.2.6 Interpreting, Creating Explanatory Accounts and Providing Meaning	77
4.3 Chapter Summary	78
CHAPTER FIVE: FRAMEWORK DESIGN.....	80
5.1 Overview.....	80
5.2 Problem Identification and Motivation.....	80
5.3 Definition of the Objectives for a Solution.....	83
5.4 Design and Development.....	84
5.4.1 Components Identification.....	86
5.4.2 Components Relationships.....	97
5.5 Demonstration.....	105
5.6 Evaluation	114
5.6.1 Objectives of the Evaluation.....	114
5.6.2 Expert Review.....	115

5.6.3 Framework Evaluation Tool	116
5.6.4 Findings of the Evaluation	117
5.6.5 Conclusion	138
5.7 Refinement of the Framework	139
5.8 Communication.....	142
5.9 Chapter Summary	142
CHAPTER SIX: FUTURE CONSIDERATIONS AND CONCLUSION	144
6.1 Overview.....	144
6.2 Research Contributions.....	144
6.3 Reflection and Lessons Learnt.....	146
6.4 Research Limitations	147
6.5 Future Considerations	147
6.6 Research Conclusion.....	148
References.....	150
Appendix A: Interview Questions	156
Appendix B: Framework Evaluation Questionnaire.....	158
Appendix C: Ethical Clearance.....	169
Appendix D: Sample – Data Collection Permission Letter	170
Appendix E: Participants’ Consent Form	172
Appendix F: Language Editor’s Report.....	174

LIST OF FIGURES

Figure 2.1 NIST Cybersecurity Framework	19
Figure 2.2 CPMI-IOSCO cybersecurity framework.....	21
Figure 2.3 The ISG framework.....	25
Figure 3.1 A design science research methodology (DSRM) for Information Systems research	42
Figure 3.2 Qualitative analysis process	50
Figure 5.1 Design Science Research Methodology (DSRM).....	80
Figure 5.2 Proposed Namibia Banking Cybersecurity Framework (NBCF).....	104
Figure 5.3 Reviewers' Demographic details: Education and Professional Certifications	118
Figure 5.4 Reviewer's Demographic details: role and experience	119
Figure 5.5 Framework relevance	125
Figure 5.6 Framework applicability.....	126
Figure 5.7 Framework suitability.....	127
Figure 5.8 Framework significance	127
Figure 5.9 Framework understandability	128
Figure 5.10 Framework components connection.....	129
Figure 5.11 Framework adoptability.....	130
Figure 5.12 Framework components changes	133
Figure 5.13 Framework components' relationship changes	135
Figure 5.14 The Namibia Banking Cybersecurity Framework (NBCF).....	141

LIST OF TABLES

Table 2.1 Cyber security standards, frameworks and best practices comparison.....	27
Table 3.1 Summary of Data collection tools	44
Table 3.2 Population sample.....	47
Table 3.3 Sample of the semi-structured interview questions	51
Table 3.4 research objectives vs research methodology	53
Table 4.1 Organised semi-structured interview questions.....	56
Table 4.2 Data Codes	62
Table 4.3 Data themes and categories.....	73
Table 5.1 Security weaknesses	81
Table 5.2 Cyber-attack types in the banking industry	82
Table 5.3 Mapping against the cybersecurity trends	82
Table 5.4 Objectives of the NBCF and significance.....	84
Table 5.5 Summary of the three selected frameworks.....	85
Table 5.6 Components relationship, importance, reference and significance	87
Table 5.7 Identified cybersecurity issues.....	93
Table 5.8 Risk assessment criteria	107
Table 5.9 Risk assessment process	108
Table 5.10 Assets classification criteria.....	109
Table 5.11 Assets risk analysis	110
Table 5.12 Assets risk labelling	110
Table 5.13 Assets risk levels.....	111
Table 5.14 Assets protection levels	112
Table 5.15 Threats detection methods	112
Table 5.16 Response activities to detected security threats and attacks	113
Table 5.17 Expert Reviewers' Profiles	117
Table 5.18 Reviewers' responses on framework appropriateness and relevance	120
Table 5.19 Reviewers' comments on the appropriateness and relevance of the framework	122
Table 5.20 Reviewer's responses on framework suitability, applicability, relevance and significance	131
Table 5.21 Reviewers' framework component changes and recommendations.....	133

Table 5.22 Reviewers' recommendations.....	135
Table 5.23 Reviewers' final comments	136
Table 5.24 Reviewers' final comments	139
Table 5.25 Overview of the Namibia Banking cybersecurity Framework	Error! Bookmark not defined.

ABBREVIATION AND ACRONYMS IN THIS THESIS

Acronym/abbreviation	Description
1. AML	Anti Money Laundering
2. App	Application
3. ATM	Automated Teller Machine
4. BID-30	BoN Determination of Information Security
5. BoN	Bank of Namibia
6. CEH	Certified Ethical Hacker
7. CERT	Computer Emergency Response Team
8. CGEIT	Certified in the Governance of Enterprise
9. CGTF	Corporate Governance Task Force
10. CIS	Center for Internet Security
11. CISA	Certified Information Systems Auditor
12. CISM	Certified Information Security Manager
13. CISO	Chief Information Security Officer
14. CISSP	Certified Information Systems Security Professional
15. CISWG	Corporate Information Security Working Group
16. CMSPSM	Common Minimum Standards of Protective Security Measures
17. COBIT	Control Objectives for Information and Related Technology
18. CPMI	Committee on Payments and Market Infrastructures
19. CRISC	Certified in Risk and Information Systems Control
20. CRM	Customer Relationship Management
21. CSIRT	Computer Security Incident Response Team
22. DMZ	Demilitarized Zone
23. DDoS	Distributed Denial of Service
24. EFT	Electronic Funds Transfer
25. EFTA	Electronic Fund Transfer Act
26. ETA	Electronic Transactions Act
27. FIA	Financial Intelligence Act
28. FFIEC	Federal Financial Institutions Examination Council
29. FTC	Federal Trade Commission
30. GDP	Gross Domestic Product
31. GDPR	General Data Protection Regulation
32. GRN	Government Republic of Namibia
33. ICT	Information and Communication Technology
34. IDS	Intrusion Detection System
35. IEC	International Electrotechnical Commission
36. IOSCO	International Organisation of Securities Commissions

37. IPS	Intrusion Prevention System
38. ISMS	Information Security Management System
39. ISSA	Information Systems Security Association
40. ISO	International Organization for Standardization
41. IT	Information Technology
42. ITIL	Information Technology Infrastructure Library
43. KYC	Know Your Client
44. MICT	Ministry of Information and Communication Technology
45. NBCF	Namibia Banking Cybersecurity Framework
46. NIST	National Institute of Standards and Technology
47. PCI-DSS	Payment Card Industry Data Security Standard
48. PMP	Project Management Professional
49. POLP	Principle of Least Privilege
50. POPI	Protection of Personal Information
51. SIEM	Security Information and Event Management
52. SSO	Single Sign On
53. WACS	West Africa Cable System

CHAPTER ONE: INTRODUCTION

1.1 Background

Information and Communication Technologies (ICTs) have become a fundamental part of everyday life for the world's most population, with its penetration moving from 6% in the year 2000 to 43% in the year 2015 in business and personal lives, and with a projected 5% yearly increase (ITU, 2016). ICTs have become a crucial component powering development, creativity and economic growth in even the world's most underdeveloped areas (World Bank, 2017). Computers are now used in almost every part of our lives, including aerospace, business, education, government, defence system, banking, and health-care.

ICTs provide significant benefits, but they are also risky, due to the ease of accessing data and using it for illegal reasons (World Economic Forum, 2020). The number, complexity, magnitude and impact of cyber-attacks have all increased (World Economic Forum, 2020). As the world grows more inter-reliant and hyper-connected, there is a growing concern about the Internet's vulnerabilities, an infrastructure that supports practically all financial operations, including commerce and the whole financial system.

Namibia is not left out in this delicate situation as she has adopted technology to drive service delivery and economic development. Due to the West Africa Cable System (WACS) connectivity of May 2012, Namibia managed to get good network communications and the country's Internet services have become well provisioned. As the Internet use expands, so does a new type of crime, cybercrime (Wall, 2015). The Namibian banking sector does not currently have an officially recognised cybersecurity framework to safeguard online transactions of financial data between banks and customers. This is due to lack of governance, supporting systems, processes and procedures to mitigate online transactions cyber threats. For example, Standard Bank of Namibia was hacked in May 2017, which resulted in 1600 fake credit cards being issued in an interval of two hours, totalling a loss of

N\$300 million (Olivier, 2017). According to Kaspersky (2020), Namibian banks are the target of roughly 2.9 percent of malware attacks worldwide. Kaspersky (2020) further states that Namibia globally ranks third in terms of malware attacks on its banking sector.

In modern times, banking institutions have adapted modern advances of doing business electronically. In Namibia, all banks to date have implemented electronic banking and mobile banking in one way or the other. As a result of technology evolution, technologies such as on-line banking and e-commerce have resulted in financial transactions amounting to millions of dollars happening across network connections, in the cyberspace, increasing the risk of Internet computer fraud in the banking sector due to online banking services (Bhasin, 2015).

By doing business in a more connected world and providing more digital products, this increases the banks' risk of successful cyber-attacks and it is not about if an attack will occur but when it will occur. The risk is thus increased on the back of the Fourth Industrial Revolution because of the disruptive impacts on technologies which entail the use of emerging technology-driven banking services (Rahman & Abedin, 2021). Therefore, the evolving of technology and the digitalisation of the bank's business processes, protecting the bank's asset data has, therefore, become a major driving force for the need for safeguarding online transactions. Thus, there is a need for the Namibian financial sector to initiate and adopt a cybersecurity framework to safeguard online transactions.

1.2 Problem Statement

As Namibian banking institutions become ever more reliant on the cyberspace to conduct business; they are increasingly being exposed to cyber threats. There is currently no documented evidence of the existence of a recognised cybersecurity framework to safeguard online transactions of financial data between banks and customers in the banking sector (Bank of Namibia Annual Report, 2017). The only security guidelines currently present are the Common Minimum Standards of Protective Security Measures (CMSPSM) that were developed for manual-based systems of the Namibian Public Service (GRN, 1996).

There is, therefore, an urgent need to develop a cybersecurity framework that can serve as guidance to safeguard online transactions of financial data between banks and customers. Thus, the current research developed a cybersecurity framework to assist banking institutions in safeguarding the transactions of online financial data between banks and customers.

1.2.1 Research Objectives

The main objective for this research was to develop a cybersecurity framework to guide Namibian banking institutions in safeguarding online transactions of financial data between banks and customers.

Sub Objectives:

- i. Assess the various patterns of cybercrimes associated with online transactions in the Namibian banking institutions' cyberspace;
- ii. Evaluate existing cybersecurity frameworks; and
- iii. Develop a cybersecurity framework to guide Namibian banking institutions in managing online financial transactions.

1.2.2 Research Questions

The research main question was; how can identified elements be used to formulate a cybersecurity framework to guide the Namibian banking institutions in managing online financial transactions?

Sub questions:

- i. What are the various patterns of cybercrimes associated with online transactions in the Namibian banking institutions' cyberspace?
- ii. What are the components/elements of existing cybersecurity frameworks and what are the missing components/elements in the Namibian context?

- iii. How can identified elements be used to formulate a cybersecurity framework to guide the Namibian banking institutions in managing online financial transactions?

1.3 Significance of the Study

This study is significant as it complements the current Namibian government initiatives and the long-term goals of Vision 2030 such as the strategy of attaining infrastructure development as stated in the Harambee Prosperity Plan, which highlights the urgent necessity to invest in cybersecurity (Harambee Prosperity Plan, 2016). The high possibility for deploying potential ICT services in Namibia as per the Harambee Prosperity Plan, therefore calls for highly concerted approaches and efforts from all stakeholders to ensure cyber-safety. This research is one of the initiatives as it can assist the banking sector in creating measures that assist growths in cybersecurity.

Furthermore, a cybersecurity framework can assist banking institutions in Namibia by providing the context on how these banks view cybersecurity risk management. Developing a banking sector cybersecurity framework will aid in unifying the processes and guiding the banks on standard requirements, which would be an important contribution to the knowledge on cyber risks and strategies in Namibia. It will also support banking institutions in considering the appropriate level of rigor for their cybersecurity programs.

1.4 Justification of the Study

The increase of cyber-attacks worldwide has put pressure on most organisations specifically the banking sector to have security measures to protect organisation's information. Banking institutions need to recognise that the traditional ways of protecting their assets and their customer's data is no longer sufficient for them to survive and be competitive in the current era where many organisations are suffering attacks by hackers in a persistent way. By doing business in a more connected world and providing more digital products increases the risk of a successful attack and that, it is not if an attack will occur but when it will occur. Thus, the

cybersecurity risk is increased on the back of the Fourth Industrial Revolution. Banks therefore need to be on their guard more than most businesses as they have high public-facing products and services. This is due to their key role in settlement and payment systems, as well as the high volume of sensitive customer information that they process. Customers are increasingly looking to banks to provide services through digital channels; therefore, a sound cyber risk management could be a key competitive differentiator for all banks in Namibia to strengthen trust and reputation. This study thus aims at developing a Namibia Banking Cybersecurity Framework (NBCF) with the ultimate objective to build cyber resilience, where systems and operations are designed to detect cyber threats and respond to and recover from cyber events to minimise business disruption and financial losses.

1.5 Delimitation

Cybersecurity is a broad topic; however, the study focused on designing a cybersecurity resilience risk management framework in the banking sector by performing a systematic review of the existing cybersecurity frameworks and standards and by the use of interview findings. There could however be different approaches to designing a cybersecurity framework such as performing studies using a cyber-threat lens, which may reveal a better understanding of crucial indicators for the framework. It should also be noted that there could have been many ways of promoting cyber resilience in the banking sector but the present study's focus was on cybersecurity framework.

1.6 Thesis Outline

The following is how the rest of the thesis is organised:

Chapter 2: This chapter summarises existing literature on patterns of cybercrimes in the banking sector, cybersecurity risks, and existing information/cybersecurity frameworks and standards.

Chapter 3: This chapter presents the research methodology utilised to attain the study objectives and answer the research questions as mentioned in section 1.2.1 and 1.2.2. It

further presents the research paradigm, the research design, the research population, sample, data collection tools, data analysis and ethical considerations.

Chapter 4: This chapter examines the data from the semi-structured interviews as well as the study's outcomes and findings.

Chapter 5: This chapter presents the steps followed in designing the proposed framework. It also provided the framework evaluation and presented a scenario of the demonstration of the framework.

Chapter 6: This chapter is a conclusion of the study with recommendations, research limitations, future work and lessons learnt.

1.7 Chapter Summary

This chapter established the study's context. The research problem statement, research objectives, research questions, study significance and the thesis outline were also addressed in this chapter. The following chapter goes over the research literature.

CHAPTER TWO: LITERATURE REVIEW

2.1 Overview

The first section provided a background to the cyber-world and cybersecurity. In this section, the cybersecurity concept is defined, explained and unpacked to further recognise the fundamental of the study issues. A comprehensive literature review was conducted with the aim of understanding the nature of cybersecurity. Furthermore, an analysis was done on the different existing cybersecurity frameworks and then a chapter summary is presented.

2.2 An Overview of Cybercrime

Today, millions of internet users all over the world have fallen victim to cybercrimes (Khan, 2018). Cybercrimes are currently the biggest threat to the banking institutions across the world, leading to massive losses of billions of dollars. Banks have high public-facing products and services among the banking institutions and thus they have become attractive targets for cyber-attacks. This is due to their key role in settlement and payment systems, as well as the high volume of sensitive customer information that they process (Khan, 2018). This has therefore necessitated a focused demand on the need to strengthen cybersecurity through adequate governance, procedures, processes and system descriptions to mitigate cyber-risks (Crisanto & Prenio, 2017).

As the global COVID-19 epidemic continues to destabilise global health and economies, another unseen threat is emerging in the digital space; cyberattacks, which are aggravated by the greater reliance on digital tools. According to the World Economic Forum (2020), most organisations are enforcing the “work from home” regulations in reaction to the coronavirus pandemic which entails that digital communication has become the new normal. As a result, most attackers take advantage of the fact that most people work remotely and that companies have not implemented the same security measures on their networks as they would in a corporate setting. Thus, cybercriminals are using coronavirus as a vector for attacking companies such as using COVID-19 “themed” phishing emails to trap people into

clicking on dangerous links that download malwares on their devices (World Economic Forum, 2020). A 2020 report by ZDNet found that COVID-19 is credited for a 238% rise in cyberattacks against banks in 2020 (ZDNet, 2020).

The global COVID-19 pandemic has altered people's working habits. Adapting to the new reality introduced by COVID-19 has been a huge problem for businesses all over the world, especially the banking sector. This, from a technological standpoint, entailed companies making massive changes of ensuring that all tools required are present to connect the entire workforces working from home. The COVID-19 crisis has forced banking institutions to increase their digital offerings, improve their online banking services and expand their digital touchpoints with their customers. Banks are reminding their customers to make use of their digital platforms to limit the spread of the virus through social distancing. As a result of this greater reliance on digital technologies, the global COVID-19 pandemic increases the risk of cyberattacks (World Economic Forum, 2020).

2.3 Global Current Cybersecurity Attacks in the Banking Sector

The following are some of the current cybersecurity weaknesses in the banking sector:

- **Mobile and Web Banking security**

Mobile and Web Banking provides a greater convenience to users but these technologies suffer from various types of attacks particularly malware attacks (Yildirim & Varol, 2019). According to the ZDNet report of 2018, Bank web apps are the most vulnerable to getting hacked.

- **The use of third parties**

The use of third parties fosters risk on the security of data. Reliance on services from third-party providers has resulted in a situation where banking systems are at risk. According to Verizon's 2019 Data Breach Investigations report, the banking sector is among the most

targeted of data breaches across all industries in 2018. As data is transferred between two different entities, third parties can impair financial institutions' security defences.

- **Compliance**

According to the Security Intelligence report 2016, compliance plays a pivotal role in ensuring that financial organisations resolve the issue of cybersecurity. Due to the ever increasing data breaches, financial organisations are now challenged with multiple views on compliance obligations on data protection and privacy (Security Intelligence Report, 2016).

- **Insider vulnerabilities**

Another cybersecurity threat in the banking sector is insider vulnerabilities. This is where users or employees within the organisations unconsciously leave the organisational data open to attacks. According to IBM's 2019 X-Force Intelligence Index, insiders fell for phishing emails and websites over two-thirds of the time, which is equivalent to 29% of attacks studied. Other common causes of insider vulnerabilities can be the improper configuration of applications and systems.

- **Large user population**

Nowadays most banking institutions are characterised by a large and complex number of users (customers and employees) accessing banking and finance networks, thereby opening new and numerous points of attacks. As a result, banks have little control over how these users interact.

- **Gaps in technology**

A 2018 report by ZDNet found that financial and banking institutions' websites are highly vulnerable to hacking. The report noted that 80% of banking sites evaluated were susceptible to cross-site scripting attacks. Therefore, apps and systems should be assessed for vulnerabilities before going live (ZDNet, 2018).

Due to security weaknesses mentioned above, the banking sector mostly suffers from the following security attacks:

- **Phishing attacks**

Phishing is a sort of cybersecurity attack that is frequently used to obtain user data, such as login credentials and credit card numbers among others. Phishing is characterised by an attacker tricking an unsuspecting victim into opening a spoofed email or link, which ultimately results into an installation of malware which can encrypt data as part of a ransomware attack.

- **Ransomware**

Ransomware is a type of malware that encrypts the files of its victims. The attacker then demands a ransom from the victim in exchange for restoring access to the data. Banks remain a popular target for ransomware attacks, as cybercriminals are looking for large pay-outs. Financial services, after healthcare, are the second most targeted industry for cyber-attacks, according to a Kaspersky Labs 2019 report.

- **Insider Attacks**

Insider threats, privacy, responsibility and trust have a massive impact on cybersecurity in all industries including the banking industry. According to Yaseen (2016), financial institutions are particularly vulnerable to insider threats because of the extremely sensitive information maintained and the strong reliance on information technologies. Yaseen (2016) further states that the financial sector is primarily affected by cases of fraud and intellectual property theft done by malicious insiders.

- **Distributed Denial of Service (DDoS)**

The banking industry is a well-known target for DDoS assaults at the network and application layers. According to the EMEIA Cyber Centre of Excellence report, DDoS attacks are used as ways of disrupting financial services. The complexity of these attacks continue to increase.

DDoS attacks have increased by an enormous 16% from November 2017 to April 2018, according to the State of the Internet 2018 report by Akamai (2018).

The above highlighted global cybersecurity attacks are also evident in the Namibian banking sector. According to Kaspersky (2020), Namibian banks are the target of roughly 2.9 percent of malware attacks globally. Kaspersky (2020) further states that Namibia globally ranks third in terms of malware attacks on its banking sector. As per the *Bank of Namibia annual report (2017)* Electronic Funds Transfer (EFT), the total fraud value amounted to N\$ 528,000 and cheque streams fraud value amounted to N\$ 2.07 million. Credit card fraud, computer fraud and manipulation of Automated Teller Machines (ATMs) fraud are the most common types of fraud experienced by banking institutions in Namibia (Bank of Namibia Annual Report, 2019).

2.4 Impact and Growth of Cybercrime on the Banking Sector

Advances in technology have provided substantial benefits and innovations to the world in massive ways (Erastus, Jere, & Bhunu Shava, 2017) such as e-commerce, timely business processing, connectivity, easy access to information, and fast communication. Such benefits and innovations have been adopted in the banking sector, for example; mobile banking, credit cards, as well as Internet banking (Umanilo et al., 2019). Innovations in the banking sector such as those available in ATMs, mobile and online banking are also noticeable and happening at a fast pace in the Namibian banking industry. For example, Bank Windhoek in February 2021 released its new mobile banking application (app) in response to their customers' needs for seamless digital banking services (Bank Windhoek, 2021).

Although IT has provided substantial benefits mentioned above it, however, comes with disadvantages such as information security breaches and unsecure ICT environments (Erastus et al., 2017). Due to the immeasurable benefits of the Internet, several end-users are now connected to the Internet, including cybercriminals, resulting in illegal activities committed over the Internet. In addition to that, advances in technology have led to a growth in

cybercrimes such as credit card theft, hacking sites and account breaches through internet banking facilities (Umanailo et al., 2019).

As a result, end-users are now connected to the Internet and this has resulted in several internet users becoming victims of cybercriminals. Due to modern ways in which organisations are operating, organisations have replaced paper-based transactions with electronic transactions which include the exchange of information in cyberspace. Services such as Internet banking and e-commerce transactions are conducted over the Internet, in cyberspace, which does not have any physical boundary limitations (Umanailo et al., 2019). According to The Global Risks Report (2018), cyber-attacks are amongst the top five ranked global risks affecting the world by perceived likelihood. In addition to that, ransomware has been identified as the main malware threat affecting organisations today and this trend is anticipated to continue over the coming years (Borrion & Yuryna Connolly, 2020).

The banking industry depends heavily on technology and thus most of the banks have digitalised their business processes, however protecting banks' asset data has, therefore, become a major driving force for cybersecurity regulation (Mohammed, 2018). The banking industry must develop a cybersecurity framework that supports banking business processes in order to mitigate cyber threats. This cybersecurity framework requires a different security mind-set and different approaches to business processes including risk management and mitigation. The ultimate result will be a robust cybersecurity framework and effective laws that promote bank-customer confidence. Some of these measures include laws such as the Electronic Fund Transfer Act (EFTA) and bodies like the Federal Trade Commission (FTC) that serve these interests.

In an effort to start to mitigate this risk, banks need to respond and adapt to the changing cyber risk landscape by implementing security measures to protect and increase their resilience to cyber-attacks. Banks must make investments in technology, people, internal processes, third party vulnerability management, threat intelligence and responsiveness.

Most banks in Namibia have therefore implemented security measures such as incident response, training and awareness, asset management, third party cyber risk management, vulnerability management (*Bank of Namibia BID-30 Information Security, 2017*).

2.5 Internet Use in Namibia

According to the *Internet World Stats Report (2020)*, Namibia's total number of Internet users reached an estimate of 1 347 418 by December 2020, whereas the Internet users growth percentage of Namibia is 4,391 percent from 2000 to 2021.

Namibia has improved its telecommunications infrastructure, solutions and services from the mid-1990s to date, and since May 2012 it has also been connected to the West Africa Cable System (WACS), which is a connection designed for high-capacity broadband, Internet access and services in the country (*Telecom Namibia Annual Report, 2016/2017*). To add to that, the improved and growth of the mobile network has led to better communication among Namibians which has resulted in easy access to Internet services through which users can do Internet payments and transfers as well as mobile banking (*MTC Annual Report, 2016*). Cybersecurity, therefore, contributes to the ongoing development of Internet infrastructure, Internet services and Information Technology (IT).

2.6 Cybersecurity Policy and Strategy in Namibia

In Namibia at present, there is no official national cybersecurity strategy (Dutton, Goldsmith, Saunders, Varese, & Von Solms, 2019). However, in February 2020, the Ministry of Information and Communication (MICT) with the assistance of the Commonwealth Secretariat, devised some of the components of the cybersecurity strategy. The Namibian government is thus in the process of finalising its cybercrime related legislation which includes the draft Cybercrime Bill and the draft Data Protection Bill. The Electronic Transactions Act (ETA) was approved in 2019 and implemented in 2020 (Ministry of Information and Communication Technology, 2020). In addition to that, the only officially recognised electronic transactions and cybercrime bill in its current draft state has a provision

of the government to monitor and/or verify agencies that need access to data which might be challenging. The bill requires organisations to lower some of their security standards in order to comply with the bill and also the fact that organisations are financially liable for data loss although the government is the governing body. As a result of the lack of cybersecurity laws, ever-advancing technologies, legal certainties, and questions of jurisdiction as there is currently no law that is guiding the bill and the poor implementation of the ones in existence, Namibia has become an international safe haven for cybercriminals. This has resulted in a large number of cybercriminals to roam freely in the country.

Namibia presently does not have a national Computer Security Incident Response Team (CSIRT) as a central registry of all the national cyber incidents which would aid in coordinating the reporting and management of the national cybersecurity incidents in the country. However, Namibia has a Computer Emergency Response Team (NAM-CERT), which is a working group established to coordinate the initiatives of the establishment of the national CSIRT in Namibia. The NAM-CERT project team has taken initiatives to establish the national CSIRT in Namibia. The draft cybercrime bill, in chapter 2, sets out specific provisions of the CERT, namely the establishment of the national CSIRT and its management committee (Dutton et al., 2019). This is the reason why a guideline for safeguarding the Namibia cyberspace is needed.

The increasing cyber threats places sensitive data and organisational security at risk. This lack of cybersecurity measures and best practices make companies easy target of hackers. According to Kaspersky (2020), about 2.9 percent of malware attacks globally targeted Namibian banks. Namibia is lagging behind in cybersecurity international trends and policies and it does not have the technical nor financial ability to deal with the threats. This has therefore necessitated the need of a cybersecurity framework as this will go a long way to curbing the menace of cybercrimes.

The financial industry regulatory authority has embarked on compliance projects for security standards, to be specific, the Payment Card Industry Data Security Standard (PCI-DSS). Besides, the financial institutions are not required to apply any specific cybersecurity standard but they can decide which ones to apply for themselves. Hence, for the financial sector of Namibia, the Bank of Namibia (BoN) which is a government body with oversight for the financial sector, requires through the policy that regulated entities can mitigate their exposure to risks and damages related to cybercrime (*Bank of Namibia BID-30 Information Security, 2017*). In an effort to start regulating the cybersecurity risk, BoN issued BID-30 which is very narrow and focuses on the traditional information security controls and does not consider the internationally recognised frameworks and standards. It also does not cover the broader umbrella concept of cyber resilience.

According to *Bank of Namibia Determination of Information Security (BID-30) (2017)*, BoN does not advocate specific information security standards to be used by banking institutions. Banking institutions should use applicable industry information security standards and sound international best practices as suitable. BoN, therefore, requires that all regulated entities can identify, measure and mitigate their exposure to risk and damages associated with cybercrime. Each banking institution is also required to guarantee that its staff, customers and suppliers are aware of cyber-crime related risks. This is achieved through staff training programmes and awareness campaigns for clients and suppliers (*Bank of Namibia BID-30, 2017*). In general, the financial sector knows that there is a huge challenge around cybercrime.

It is therefore important for BoN to have proper co-ordination among regulators to ensure a comprehensive and consolidated bank view of its activities and legislation. Cybercrime does not only impact victims, but it also has long term impacts. For example, cybercrime can impact the daily activities of end-users such as an inability to receive up-to-date information and doing financial transactions like withdrawing cash from ATMs. In addition to that, cybercrime may result in leaking of information to unauthorised bodies and lastly loss of

intellectual property which can affect companies' competitive advantages with other businesses (Mohammed, 2018). As there are now massive investments in e-Government initiatives by the government of Namibia, there is a need for proportional investments in the network security framework. Therefore, the cyber security best practices must be developed not only for the general public but also for financial institutions.

This lack of cybersecurity measures and best practices make companies easy targets of hackers. While legislation on cybercrime was generally concentrated in developed countries, the influence of the Internet on cybercrime should be speedily considered in legislation even in less developed and developing countries (Li, 2017). Law enforcement should also take a series of measures against cybercrime. Namibia is however behind in cybersecurity international trends and policies and it does not have the technical nor financial ability to deal with the threats. This is, therefore, the reason why a cybersecurity framework is needed as this will go a long way to curbing the menace of cybercrimes.

2.7 Existing Cybersecurity Frameworks, Best Practices and Standards

2.7.0 Introduction

The dynamics of cyber threats on banks is a major risk and this has urged the need to strengthen cybersecurity in the banking sector. Thus, cyber risk is every bank's concern. Cyber risk can be defined as "operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems" (Bouveret, 2018, p. 4). Cybersecurity is therefore the process of protecting information and technology assets (networks and devices) from emerging risks and cyberattacks.

It is important for organisations to adopt international cybersecurity standards or best practice frameworks to oversee or provide guidance on cybersecurity. For a cybersecurity conceptual framework to be successful, there is every need to look at industry standards and

best practices (Kritzinger & Von Solms, 2012). In the same vein, there are a few standards, frameworks and best practices that have been adapted for cybersecurity (Kritzinger & Von Solms, 2012). Some of the international standards and best practice frameworks include (i) NIST cybersecurity framework for critical infrastructure (National Institute of Standards and Technology, 2018), (ii) The Committee on Payments and Market Infrastructures (CPMI) cyber security framework (Crisanto & Prenio, 2017), (iii) ISO/IEC 27001:2013 Standards on Information Security Management System (ISO (2013)), (iv) Center for Internet Security (CIS) (Center for Internet Security, 2018) and (v) a framework for the Governance of Information Security in Banking System (Ula, Ismail, & Sidek, 2011). The following sections focus on reviewing the listed frameworks.

2.7.1 National Institute of Standards and Technology (NIST) Cybersecurity Framework

The National Institute of Standards and Technology (NIST) is a framework of the United States government for improving critical infrastructure cybersecurity. According to Chochliouros et al. (2015), critical infrastructure include assets or systems which are crucial for maintaining critical national functions, and it includes physical resources, IT facilities, services, networks and infrastructure which are important to the national health and security, public safety, economy and local citizens well-being. It is crystal clear that the banking sector and or banking institutions are clearly part of the critical infrastructure since they heavily rely on ICT as their business enabler. They have a major role in providing significant support services for the economy and society, especially by increasing the country's Gross Domestic Product (GDP), and their systems security is therefore of great importance for a functioning market (National Institute of Standards and Technology, 2018).

In the year 2013, on February 12, the United States president requested NIST to develop a cybersecurity framework which is effective for protecting critical infrastructure, as per 13636 executive order of the US President (Order, 2013). As a result of the executive order, a NIST cybersecurity framework has been developed and published. The NIST cybersecurity framework was developed to help organisations of any size, sector and type to manage their

cybersecurity risks through aligning business risks to the cybersecurity risks (National Institute of Standards and Technology, 2018). Since the NIST framework focuses on business objectives and drivers, it assists organisations by identifying, assessing, and managing cyber-risks. There are currently no cybersecurity best practices defined, thus the NIST framework is therefore designed to shape standards for any organisation in any sector or community such as private and government sectors and not only for the critical infrastructure organisations.

There are three aspects to the NIST cybersecurity framework; the framework core, profile and implementation tiers. The framework core refers to a set of cybersecurity events which provide a set of desired cybersecurity outcomes for sectors with critical infrastructure. Five functions make up the framework's core, namely identify, protect, detect, respond, and recover as highlighted in figure 2.1. The framework profiles describe the organisation's outcomes according to unique business requirements from categories and sub-categories. Implementation tiers indicate how organisations manage cybersecurity risks and procedures to control the risks (National Institute of Standards and Technology, 2018).

Figure 2.1 presents the NIST Cybersecurity Framework.

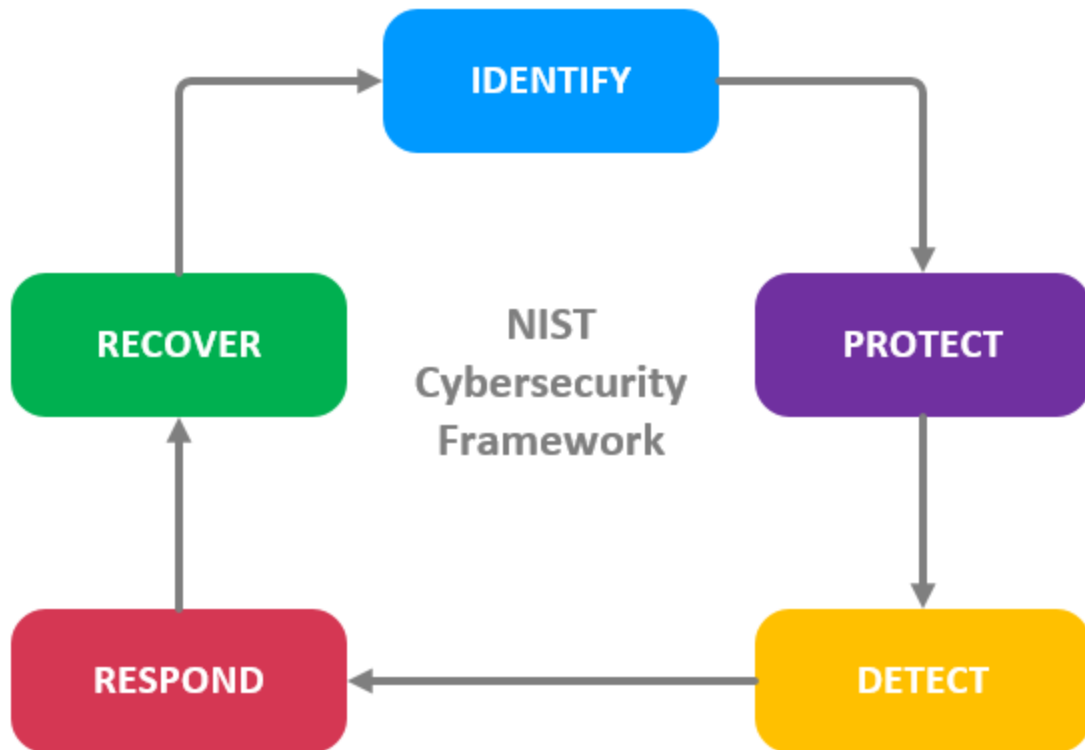


Figure 0.1 NIST Cybersecurity Framework

The NIST framework offers multiple cybersecurity approaches to organising structure through the 22 control objectives by collecting guidelines, standards, and practices that are effectively working today (Jazri & Jat, 2016). Different governments have different takes on what they define as their critical infrastructure. In Namibia, critical infrastructure has not yet been officially defined and identified. However, MICT established a multi-sectorial steering committee which identified some critical infrastructure sectors at the national level. Thirteen critical infrastructure sectors were identified, namely; (1) National Defence and Security, (2) Banking and Finance, (3) Information and Communications, (4) Energy, (5) Transportation, (6) Water, (7) Health Services, (8) Government, (9) Emergency Services, (10) Mining, (11) Food and Agriculture, (12) Space and (13) Education (Dutton et al., 2019).

How is the NIST cybersecurity framework applicable to the banking sector? The financial system is an international system and not just a domestic system. It is very crucial to

understand the international definition of critical infrastructure and how to socialise it with international regulators. It is clear that the financial sector is a complex regulatory environment and has several international compliance requirements, a good example being PCI-DSS. The NIST cybersecurity framework involves organisations setting their own level of precaution. Since it is flexible and as every organisation will have unique threats, vulnerabilities and risk factors, how they implement the framework will vary. It is therefore for this reason that the NIST cybersecurity framework is also appropriate for use in the banking sector.

The use of this voluntary framework helps in improving the cybersecurity of the critical infrastructure and guide individual organisations in increasing the cybersecurity posture, identify and prioritise scenarios for improving IT security through risk assessment, target state and assess progress in cybersecurity (Teoh, Mahmood, & Dzazali, 2017). Thus, in the banking sector, the framework could enhance cybersecurity resilience and provide improved safeguards for the banking institutions' client accounts and data.

2.7.2 The CPMI-IOSCO Cybersecurity Framework

In the United Kingdom and the United States, there are certain jurisdictions and regulatory initiatives on banks cyber-risks. The Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO) in 2016, issued regulation on cyber resilience for financial sector infrastructures (Crisanto & Prenio, 2017) for the United Kingdom and United States. According to Crisanto and Prenio (2017), “for jurisdictions with specific regulatory requirements for cyber-risk, the usual starting point, as with any other general regulation on other risks, is for banks to have a documented cybersecurity programme or policy” (p. 6). These requirements for cyber-risk therefore are based on the CPMI risk management groups.

Figure 2.2 presents the CPMI-IOSCO Cybersecurity Framework

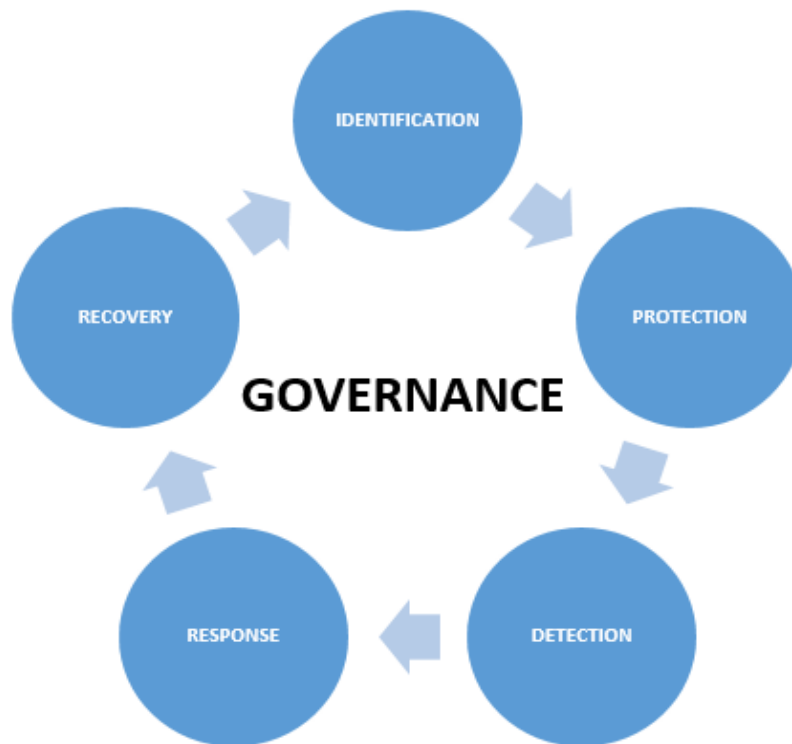


Figure 0.2 CPMI-IOSCO cybersecurity framework

2.7.3 ISO/IEC 27001:2013 Standards on Information Security Management Systems

Another prominent technical standard in the cyber and information security community is the International Organisation for Standardisation and the International Electrotechnical Commission (ISO/IEC) 27000 series. ISO/IEC 27001:2013 is a well-known expert committee that was established to develop international management systems standards for information security, also known as the implementation of an information security management system (ISMS) in organisations, and it has been implemented by many organisations world-wide (Iec, 2013). ISO/IEC 27001 has been developed for protecting organisations' information assets. The adoption of ISMS assists companies in the implementation of countermeasures to information systems-related vulnerabilities.

Risk management, security management, governance and compliance are all covered under the ISO/IEC 27001 standard. It aids organisations in ensuring that the necessary people,

procedures and technologies are in place, as well as facilitating a proactive approach to security and risk management (ISO, 2013)). A successful ISMS under ISO/IEC 27001:2013 standard requires mandatory commitments for information security from all stakeholders and top management within the organisation. These ISO guidelines are used to start, implement, maintain, and improve organisations' information security management.

For the purpose of this research, the main focus of interest is the normative references of the standard, which references control objectives and controls totalling up to one hundred and fourteen controls (114), excluding the security controls clauses' title containing main security categories and control objectives. In consideration of the organisation's information security risk environment, these controls should be reviewed and considered by organisations interested in implementing this standard. It is therefore, crucial for organisations applying the ISO/IEC 27001:2013 standard to identify applicable controls with relevance to their importance and the application to their business processes and thus any omission to these controls should be appropriately justified and documented.

Simplicity and flexibility are the main key success factors to the successful and effectiveness implementation of this standard. Therefore, it is for this reason that any organisation is allowed to perform their own process fit-in depending on the circumstances, and appropriateness of the applicable controls within their own organisation tailored on their business demands, ensuring that the total controls baseline remain the same, which is 114 controls, as per the normative references of ISO/IEC 27001:2013 standard. In this research, these 114 controls are used as a baseline for the proposed cybersecurity framework checklist.

2.7.4 Center for Internet Security (CIS)

In March 2018, CIS controls version 7 was released, which is the latest twenty important cybersecurity recommendations. The CIS controls are the in-depth-defence security best practices created by IT experts from an extensive range of sectors to mitigate cyber-attacks against systems and networks (Center for Internet Security, 2018). The current evolution of

what is referred to as cyber defence is a result of massive data losses, credit card breaches in banks, privacy threats, theft of intellectual property and denial of service. This is because we live in a digital and interconnected world, with billions of connected devices from mobile devices, personal computers to IoT devices.

CIS provides cyber defenders access to security standards, best recommendations of security controls and best practices. It looks at the most critical risk areas that organisations need to mitigate so as to enhance the organisation's current security state. The CIS controls concentrate on the most important and beneficial security activities that any organisation can implement in order to provide world-class cybersecurity solutions that prevent and respond to cyber incidents quickly. The fundamental goal of the CIS controls is to improve the organisation's knowledge and capabilities to prevent, notify, and respond to cyber-attacks.

The CIS has five critical tenets of a strong cyber-defence system namely; (1) offense informs defense, (2) prioritization, (3) measurements and metrics, (4) continuous diagnostics and mitigation and (5) automation. CIS controls version 7 has 7 key principles, and it looks at the current cybersecurity threat landscape that all organisations are encountering. It was also well aligned with other frameworks, such as the mapping to NIST Cybersecurity framework discussed in 2.7.1 above and the controls are adaptive, relevant, helpful, measurable and flexible for various organisations of all sizes considering securing its systems and data. The CIS controls V7 consist of 20 controls that organisations all over the world can adopt to remain cyber secure.

The CIS 20 controls are separated into three distinctive categories, namely; basic, foundational, and organizational. The essential controls that every organisation should implement for critical cyber defence readiness are known as basic controls. Foundational controls are a step above the basic controls, and they are technical best practices to be implemented by any organisation to ensure clear security benefits. Lastly, organisational controls are concerned with the people and procedures involved in cybersecurity.

2.7.5 A Framework for the Governance of Information Security in Banking System

Information has become the most precious asset in modern banking and it must be protected from insiders, outsiders and competitors (Ula et al., 2011). Clients are very sceptical about their privacy and thus, security has become banks' top requirement when providing banking services. Several cybersecurity frameworks have been created and widely used to date. According to Ula et al. (2011), "information security governance consists of structures, relationships and processes; the existing guidance that provides frameworks for implementing information security governance. The implementation proceeds mainly by mapping Information Security governance responsibilities to the organizational hierarchy" (p. 4).

The original design of the proposed Information Security Governance (ISG) framework is an integration of best practices and all accessible framework components. The ISG framework is an integration of several governance frameworks available today such as the Federal Financial Institutions Examination Council (FFIEC), Control Objectives for Information and Related Technology (COBIT), the International Organization for Standardization (ISO) 27002, and PCI-DSS, the Corporate Governance Task Force (CGTF), Information Systems Security Association (ISSA), and the Corporate Information Security Working Group (CISWG).

The banking sector can use the ISG framework as a starting point for governing information security by defining standards and implementing controls to protect banking information assets from cybersecurity threats. It's noteworthy that none of the frameworks address all aspects of information security governance, and others, like the PCI security standard, are particularly tailored to the operational level. Other frameworks, such as ISO 27002 or COBIT, also detail technical practice security guidelines, which are primarily concerned with the basic configuration and operation of IT systems and only indirectly concerned with data security (Ula et al., 2011, p. 5). Strategic level, tactical level, operational level, and technical level are the three levels of the framework.

Figure 2.3 presents the ISG framework by Ula et al., 2011

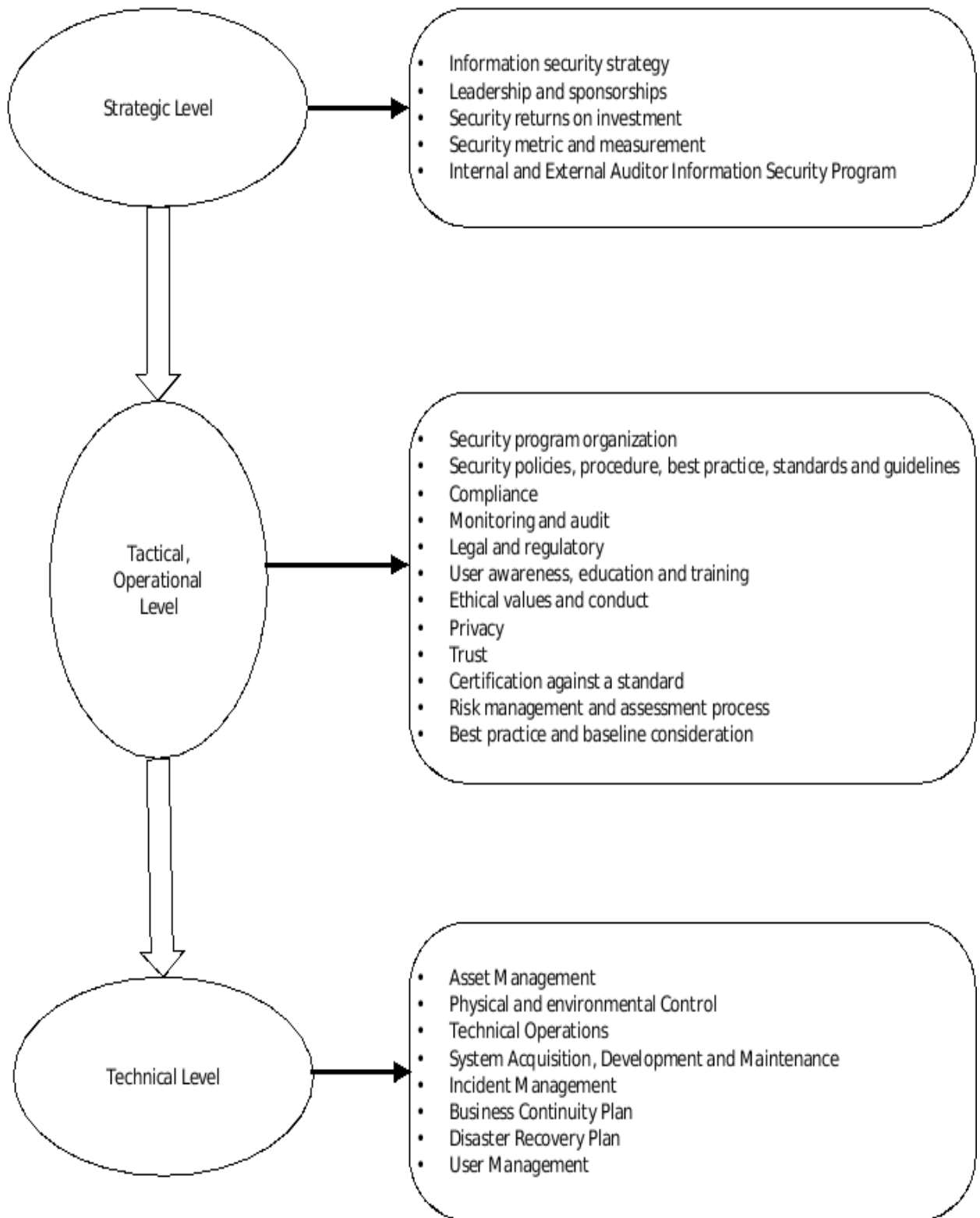


Figure 0.3 The ISG framework

Unfortunately, cybersecurity frameworks differ from country to country because of environmental and situational differences. Namibia also as a sovereign nation, needs to develop its framework that will be able to cater for the cybersecurity needs of both its citizens and its financial institutions. So how exactly is Namibia different from other countries? Namibia currently has no official national cybersecurity strategy to date (Dutton et al., 2019). In addition to that, there is no officially recognised cybercrime law or cybersecurity regulation. Namibia presently does not have a national Computer Security Incident Response Team (CSIRT) as a central registry of all the national cyber incidents which would aid in coordinating the reporting and management of the national cybersecurity incidents in the country.

According to *Bank of Namibia BID-30 Information Security (2017)*, BoN does not advocate specific information security standards to be used by banking institutions, thus banking institutions should use applicable industry information security standards and sound international best practices as suitable. BoN, therefore, requires that all regulated entities can identify, measure and mitigate their exposure to risk and damages associated with cybercrime. The above are therefore reasons why Namibia is different from other countries in terms of cybersecurity regulations and hence why there is a need to develop a specific cybersecurity framework for the banking sector of Namibia.

Though notwithstanding the differences as they affect different nations, international guidelines need to be followed while developing the national framework. Security regulations vary from country to country and Namibia is not left out. As a sovereign nation, Namibia takes the responsibility of developing its measures on how to curb the menace. Furthermore, the approach used by these criminals may also vary from country to country since there are also environmental and situational differences. Therefore, Namibia cannot adopt the cybersecurity framework of other countries because this may not be appropriate for use in the country.

Table 0.1 Cyber security standards, frameworks and best practices comparison

Cybersecurity standards, frameworks and best practices comparison	NIST (National Institute of Standards and Technology) cyber security framework	CPMI cybersecurity framework	ISO/IEC27001	Center for Internet Security (CIS)	A Framework for the Governance of Information Security in Banking System
Approach used to create the model (framework)	Risk-based iterative approach (through alignment of cybersecurity risks to the business risks)	Risk-based approach	Process-based approach	Security standards and best practices of security controls	A general approach to information security governance
Main elements used to create the model	Framework core, implementation tiers and profiles	Three primary components: - testing - situational awareness, and - learning and evolving	Plan-Do-Check-Act process cycle model	Five critical tenets for an effective cyber defence system: - offense informs defence - prioritisation - measurements and metrics - continuous diagnostics and mitigation and - automation	Information security governance frameworks, standard, best practice and guidelines

The mode of evaluation and validation	No Evaluation	No Evaluation	No Evaluation, it is used as a basis program that combines risk management, security management, governance and compliance	No Evaluation, the controls are used as in-depth-defence security best practices for mitigating cyber-attacks against systems and networks	No evaluation, it needs to be reviewed by professionals and tested in the real banking environment
Is the model sustainable?	Sustainable - provides comprehensive visibility, security and control into critical infrastructure assets and activities associated with them for organisations looking to better manage and reduce their cybersecurity risk	No sustainability as it is UK and US specific	Sustainable - most widely adopted standards because it is universal and it can be applied to any organisation regardless of its location (country), sector or size	Sustainable – security controls for cyber defence which provide specific and actionable ways to the most pervasive cyber-attacks. It also leverages real data from actual past attacks to prepare organisations for defence against future attacks. Controls can be adopted by thousands of global enterprises, whether large or small	Reflects sustainability – it is an integration of several best practices and all available framework components such as FFIEC, COBIT, ISO, PCI-DSS, CGTF, ISSA and CISWG

Does the model define deployment stages?	Yes, the framework describes different 12 deployment stages, from prioritization to cyber security life cycle management	Yes, risk management categories (Governance, Identification, Protection, Detection, Response, Recovery)	No, defines requirements and processes for establishing, implementing, reviewing and monitoring, managing and maintenance of information management system	Yes, CIS Controls are divided into three distinct categories: basic, foundational, and organizational	Yes, corporate hierarchy which are: Strategic level Tactical level Operational level Technical level
Does the model relate to cybersecurity in banking sector?	Yes, although the framework talks about cyber security for critical organisations in general, the banking sector is part of the critical infrastructure	Yes, the framework is for the cyber resilience for financial market infrastructures specifically for banks	No, it's designed for the implementation of an information security management system and not cyber security specific risks	Partially, the CIS controls are a prioritised set of actions any organization (including banks) can follow to improve their cybersecurity posture	No, it's related to information security governance

<p>What in the model addresses the banking sector (specific guideline)?</p>	<p>Alignment of cybersecurity risks to the business risks in the banking sector</p>	<p>Addresses cyber-resilience for financial sector infrastructures</p>	<p>Establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management within the banking sector</p>	<p>The five critical tenets for an effective cyber defence system</p>	<p>Govern information security by developing guidelines and implementing controls to protect banking information assets from the cyber security threats</p>
--	---	--	---	---	---

2.8 Research Gaps in the Existing Frameworks

Some information security and cybersecurity guidelines, standards and frameworks were explored above. These standards and frameworks cannot be generalised and used for the Namibian banking sector since none of them can fulfil the specific and unique needs of the Namibian banks. These standards and frameworks differ from country to country. One of the reasons this is so is because of environmental and situational differences. Namibia, as a sovereign nation, must also build a structure capable of meeting the cybersecurity needs of its population and financial institutions.

It should be noted that Namibia is different from other countries. Firstly, while other countries have national cybersecurity strategies, Namibia currently has no official national cybersecurity strategy. However, in February 2020, MICT with the assistance of the Commonwealth Secretariat, devised the components of the cybersecurity strategy. The Namibian government is thus in the process of finalising its cybercrime related legislation which includes the draft Cybercrime Bill and the draft Data Protection Bill. The Electronic Transactions Act (ETA) was approved in 2019 and implemented in 2020 (Ministry of Information and Communication Technology, 2020).

Furthermore, literature clearly revealed that the focus of the majority of the framework studies contain only few cybersecurity features such as security policies, procedures, best practices, standards, and guidelines, security programme, monitoring and compliance, user awareness, education and training, risk management and assessment processes, and no attention was given to the other essential features such as human factors and cybersecurity simulations. Some gaps exist in them and their conceptualisation of cyber risks in the banking sector hampers their adaptation in developing countries like Namibia.

Components such as corporate governance, ethical conduct, trust, and auditor security program are not included in all frameworks reviewed, although all four components are considered as important components by various researchers (Ula et al., 2011) when

implementing information security controls in an organisation. Although corporate governance is incorporated in the NIST framework and ethical conduct and auditor security programmes in the ISO standard, it's unfortunately not clear how this can be implemented in the Namibian context. Most outlines about these components or how they should be implemented are given in most European countries' compliance context and compliance to these standards is enforced unlike in Namibia. The table above gives a general comparison of the cybersecurity best practices in the most cited information and cybersecurity studies. The selected frameworks have been used in the table above to demonstrate how the existing studies have been analysed for cybersecurity characteristics.

Secondly, some of the existing cybersecurity frameworks, best practices and guidelines such as NIST, CPMI cybersecurity framework, ISO/IEC27001, CIS and a framework for the Governance of Information Security in Banking System in the literature have not undergone any evaluation (Ula et al., 2011). Framework and standard evaluation is important as it helps in assessing the usability and feasibility of these frameworks. Therefore, further research needs to be undertaken involving top management stakeholders in the banking industry. It is worthwhile to bring together these stakeholders in the banking industry particularly in Namibia to tackle these cyber risks and build a theoretical standpoint for cybersecurity, consider implementation feasibilities in the banking sector as well as ways to evaluate cyber threats and make it sustainable.

Lastly, according to *Bank of Namibia Determination of Information Security (BID-30) (2017)*, BoN, which is the regulatory authority of banks in Namibia, does not advocate specific information security standards to be used by banking institutions, banking institutions should use applicable industry information security standards and sound international best practices as suitable. BoN, therefore, requires that all regulated entities can identify, measure and mitigate their exposure to risk and damages associated with cybercrime. Each banking institution must also ensure that its employees, customers and suppliers are aware of the cyber-crime related risks (Bank of Namibia BID-30, 2017). This is therefore the reason why we

need to design a banking sector cybersecurity framework for unifying the processes and guiding the banks on standard requirements which would be an important contribution to the knowledge on cyber risks and strategies in Namibia.

2.9 Chapter Summary

The chapter presented a holistic view of cybercrimes in the banking sector. There are several types of cyber-attacks experienced in the Namibian banking sector such as credit card fraud, computer fraud, phishing attacks, ransomware, insider attacks, and DDoS attacks. The continuing digital transformation, which has increased the industry's potential attack surface is the key risk for cyber-attacks within the banking systems/ecosystems. Banks have become attractive targets for cyber-attacks because of the high volume of sensitive customer data that they process and their key role in payment and settlement systems. In an effort to mitigate this risk, banks have responded by adapting to the changing cyber risk landscape by implementing security measures such as incident response activities, training and awareness, asset management and third party cyber risk management. There are globally recognised Information/cybersecurity standards and frameworks that banks could adopt in an effort to increase their cyber resilience. Some of the international standards and best practice frameworks include NIST cybersecurity framework, the CPMI cyber security framework, ISO/IEC 27001:2013 Standards on Information Security Management System, CIS and a framework for the Governance of Information Security in Banking System. However, the available literature clearly revealed that the focus of the reviewed framework studies contain only few cybersecurity features such as security policies, procedure, best practice, standards, and guidelines, security programme, monitoring and compliance, user awareness, education and training, risk management and assessment processes. Also, it's unfortunately not clear how these frameworks can be implemented in the Namibian context. There are thus gaps identified in some of the existing information/cybersecurity standards and frameworks, as not much attention was given to the other essential components such as human factors, cybersecurity simulations, corporate governance, ethical conduct, trust, and auditor security programme hence these limitations identified from this chapter were used to inform the

proposed framework design discussed in chapter 5. The next chapter presents the research methodology that was employed to conduct the study.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Overview

This chapter focuses on the research methods used in this study. The research paradigm was deliberated to point out various aspects of this study. Also, the research design which include a qualitative method approach comprising of semi-structured interviews was applied in collecting data. To obtain reliable and valid responses, the research population, sampling procedures, data collection methods, data analysis, research procedures and research ethical considerations are also presented.

3.2 Research Paradigm

The research paradigm consists of three fundamentals: the certainty of knowledge through experience, the approach taken and principles for validity (Thanh & Thanh, 2015). There are different paradigms which are most commonly used in research such as positivism, pragmatism and interpretivism.

An evaluation of the different research paradigms reveals that positivist research is characterised by the formulation and testing of hypotheses by using exact, objective metrics and is most commonly linked with quantitative data (Muganda, 2010). On the other hand, pragmatists believe in external reality, as they believe that there are many different ways of undertaking research but do not believe a single point of view can ever give the possibility to fully determine certain concepts as there may be multiple realities (Collis & Hussey, 2013). Thus, it is difficult to fully 'unpack' causal relationships in pragmatism research. Pragmatics can combine both, positivisim and interpretivism positions (qualitative and quantitative).

Another common research paradigm is interpretivism, which is the research approach where a researcher is also intimately or subjectively involved in what is being investigated (Muganda, 2010). Interpretivist research normally creates an understanding of the perspective of social context influences as it presents a rich and complex description of a

particular context or case (Muganda, 2010). Different paradigms inherently comprise of different views; hence, they have different assumptions of reality and knowledge, which strengthens their particular research approach.

Interpretivism is the research paradigm adopted for this research. This is because it is more concerned about gaining an understanding of the social context of organisations, which includes understanding the social processes of organisations and how these social processes are interpreted or perceived by the persons in these organisations (Muganda, 2010). The research objectives do not include testing hypotheses (positivist) and also, the research intended to unpack causal relationships in regards to cyber threats and attacks, thus the reason why positivist and pragmatism were not adopted for this study.

Gray (2014) states that realism is an example of the interpretive approach whereby knowledge is advanced over theory-building process where discoveries add to what is already known. Interpretive studies are normally inductive and often connected with qualitative approaches to data gathering and analysis (Gray, 2014). With induction, the researcher starts with data collection in an attempt to develop a theory (Ormston, Spencer, Barnard, & Snape, 2014). Inductive techniques are intended to aid in the interpretation of meaning in complex data by generating summary themes or categories from the raw data, a process known as data reduction.

According to Goldkuhl (2012), interpretivism research is characterised by the type of knowledge which is gained through understanding. The role of knowledge in interpretivism is to be interesting in itself. The interpretivism method is connected to field studies and data generation is conducted through interpretation of the collected data (Goldkuhl, 2012). With interpretivism, the researcher is engaged in understanding the investigated topic which is the value of its own.

This study was thus informed by the use of the interpretivism paradigm, collected data from different sources during a field study in an attempt to assess the various patterns of cybercrimes associated with online transactions and evaluating the existing cybersecurity frameworks.

3.3 Research Design

The use of qualitative methods was adopted in an interpretive effort to assess the various patterns of cybercrimes associated with online transactions and evaluate the existing cybersecurity frameworks at different banking institutions. The qualitative research method is defined as “a research process that uses inductive data analysis to learn about the meaning that participants hold about a problem or issue by identifying patterns or themes” (Lewis, 2015, p. 473). Qualitative approaches examine the why and how of decision making, not just what, where, when, or who (Creswell & Poth, 2017).

According to Creswell and Poth (2017), qualitative research can be carried out using different methods to meet different needs, such as observation, interviews, surveys, content analysis and network research. The qualitative research method enables the researcher to have an in-depth and holistic understanding of the research field (Gray, 2014) hence why it is suitable for this study. Semi-structured interviews were employed in the study since they are non-standardised and are commonly used in qualitative analysis. For this study, qualitative research methods were used as they provide in-depth knowledge of the proposed study.

With the adoption of qualitative research design, semi-structured interviews were used to study various patterns of cybercrimes associated with online transactions and evaluate the existing cybersecurity frameworks in banks as this assisted in understanding of the as-is state of cyber maturity and identifying areas of improvement in the banks. Semi-structured interviews were chosen as the best strategy for this study since they allow for the rephrasing

of interview questions. They also allow the interviewer to probe as much as they can until they obtain answers more relevant to the study (Doody & Noonan, 2013).

Qualitative data were obtained through interviews carried with staff from the different banks in Namibia. Interviews and discussions were performed with the staff to obtain qualitative data.

3.4 Data Collection

Qualitative research data collection instruments associated with the interpretivist research include interviews, observation, content analysis, focus group and discussions. These research methods allow for inductive analysis and they are valuable in answering the initial research question(s) on the research being carried out, ultimately achieving the research objectives. To achieve these objectives, several data collection tools were used as detailed in the following sections:

Objective 1: Assess the various patterns of cybercrimes associated with online transactions in the Namibian financial institutions' cyberspace

There are several data collection tools for interpretive research that the researcher can select from such as observations, focus groups and discussions as well as interviews. The focus group discussions are one of the many types of data collection techniques. They primarily comprise of a group of participants coming together in small groups of between four and twelve participants where interactions take place (Saunders, Lewis, & Thornhill, n.d.). The two main characteristics of the focus group that differentiate them from other data collection techniques are its use of a moderator who leads the discussions and the interactions that arises during the debate (Acocella, 2012). Focus groups are normally adopted because they are considered to be an easy-to-organise and non-expensive technique but not necessarily because it is suitable for achieving the research goals (Acocella, 2012).

Observations are a systematic review of participants' actions and the recording, analysis and interpretation of the observed events (Gray, 2014). Observations allow the researcher to eliminate the subjective bias and obtain information which relates to what is currently happening (Kothari & Garg, 2014). The disadvantages of observations are that the information provided by observations are limited and at times unforeseen factors interfere with the observational task (Kothari & Garg, 2014). Observations are mainly used in studies relating to behavioural sciences.

Another common data collection tool for interpretive research is a structured or semi-structured interview. With the structured interviews, all respondents answer the same question to give all interviewees the same context of questioning (Gray, 2014). The strengths of structured interviews are the use of a detailed interview guide which allows the topics and the format of the interview to be controlled by the researcher (Saunders et al., n.d.). The researcher needs to strictly adhere to the predetermined questions with structured interviews and this might hinder the researcher on accessing participants perspectives and understanding of the researched topic (Merriam & Tisdell, 2016).

Semi-structured interviews are not standardised and are typically used in qualitative research. According to Doody and Noonan (2013), semi-structured interviews entails using predetermined questions, of which the researcher is allowed to seek clarification. Therefore, to achieve objective 1, semi-structured interviews were adopted in this study. This is because semi-structured interviews allow the interviewer to delve further into the interviewee's comments while staying within the study's parameters and goals (Alshenqeeti, 2014). The rest of the tools described above were not suitable for use because they fail to help in achieving this research objective.

For the semi-structured interviews, an interview guide was developed based on the research objectives informed by literature. However, since the interview was flexible and had open-ended questions, additional questions were asked which provided a chance to explore issues

that arose spontaneously, which made it suitable for this study. In addition to that, the order of the interview questions and wording of the questions could easily be changed depending on the direction of the interview as well as the interviewer's discretion (Doody & Noonan, 2013).

Before data collection, the researcher applied for research ethical clearance from the university which was adopted for ethical issues (refer to appendix C). Once the interview guide was designed it was shared with supervisors for content reviewing and flow error checking. Thereafter, the interview questionnaire convergence was performed to ensure that it is adequate enough in achieving the research objectives and answering the research questions. Afterwards, it was pre-tested with three peers who were fellow research students in the cybersecurity field to gauge time, reconstruct questions and test appropriateness. Subsequently, the final tool was then deployed to the sample.

Five participants were interviewed face to face and the other three were interviewed via Microsoft teams. Before the interview commenced, the researcher introduced herself to the participants and the participants introduced themselves as well. After the introduction, each participant was handed a consent form which they have signed together with the researcher (refer to appendix E). The interview sessions were about 20 minutes long and the researcher took notes during the interview and used a digital audio recorder to record the interview sessions.

With a semi-structured interview, the interviewer was able to probe for more details as much as possible until she acquired answers more relevant to the study. This is one of the strengths that semi-structured interviews provide in achieving the research objectives. Moreover, the researcher was free to give explanations or rephrase questions to respondents if they were found to be unclear and she was also able to seek for clarification where the responses were not clear (Doody & Noonan, 2013).

Through the semi-structured interviews, open-ended questions were used to obtain data, which were grouped into themes and categories. Interview questions were derived from the research problem. The interviews were done face to face and the researcher used a voice recording device. The participants gave consent and thus the interviews were recorded and their interview out-puts are audio records. The audio recordings were later transcribed. The interview was designed using literature and research objectives (refer to appendix A for the interview guide design protocol). This was important in achieving objective 1, assessing the various patterns of cybercrimes associated with online banking transactions in the Namibian cyberspace.

Objective 2: Evaluate existing cybersecurity frameworks

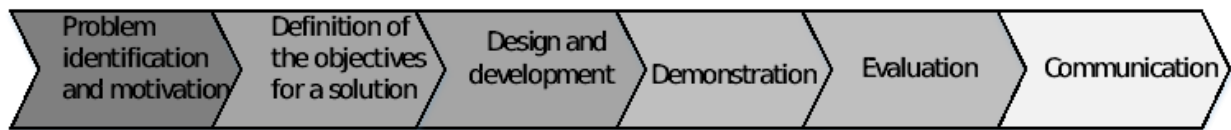
To achieve objective 2, the literature review was used as the main source for evaluating the existing cybersecurity frameworks. Existing cybersecurity best practices, guidelines and frameworks were systematically reviewed for guidance in the development of the cybersecurity framework. In addition to a literature review, face to face semi-structured interviews with bank staff were employed to find out if banks have adopted some international cybersecurity standards and frameworks and seek feedback on how they have adjusted them to fit their enterprise needs. This review assisted in identifying gaps in these frameworks which were filled by this study.

Objective 3: Develop a cybersecurity framework to guide Namibian banking institutions in managing online financial transactions

Ellis and Levy (2010) define design and development research as a well-organised study performed to develop a program or product to improve what is being developed or the developer. There are different types of design methodologies that a researcher can choose from, i.e. design science research and design engineering research.

According to Peffers, Tuunanen, Rothenberger, and Chatterjee (2007), “design science creates and evaluates IT artefacts intended to solve identified organisational problems. It involves a rigorous process to design artefacts to solve observed problems, to make research contributions, to evaluate the designs, and to communicate the results to appropriate audiences” (p. 6). Whereas, design engineering research aims at developing knowledge (Blessing, Chakrabarti, & Wallace, 1995). To achieve objective 3, a design science research methodology (DSRM) for Information Systems research by Peffers et al. (2007) was adopted. This approach was adopted to produce an artefact (cybersecurity framework) which was shaped to address the cyber threat problems in the banking sector of Namibia.

The design science research methodology by Peffers et al. (2007) consists of six steps, as shown in figure 3.1.



A design science research methodology (DSRM) for Information Systems research

Figure 0.1 A design science research methodology (DSRM) for Information Systems research

i. Problem identification and motivation

According to Kaspersky (2020), nearly 2.9% of malware attacks globally are targeted towards Namibian banks. Kaspersky further states that Namibia globally ranks third in terms of malware attacks on its banking sector. Nevertheless, the Namibian banking sector does not currently have an officially recognised cybersecurity framework to safeguard online transactions of financial data between banks and customers, this is due to lack of appropriate governance, supporting systems, procedures and processes to manage cyber-risks associated with online transactions. Thus, there was a need to develop a cybersecurity framework that can serve as guidance to safeguard online transactions of financial data between banks and customers. The design of the framework was based on data of the assessment of the various patterns of

cybercrimes associated with online transactions and evaluating the existing cybersecurity frameworks.

ii. Definition of the objectives for a solution

The objective was to develop a cybersecurity framework to guide banking institutions in safeguarding online transactions of financial data between banks and customers. The need to adopt other international frameworks as there are environmental and situational differences was a concern. Security regulations also vary from country to country and Namibia is not left out. As a sovereign nation, Namibia takes the responsibility of developing its measures on how to curb the menace. Therefore, Namibia cannot adopt cybersecurity framework of other countries because it may not be appropriate for use in the county. This is, therefore, the reason why a cybersecurity framework was needed as this will go a long way to curbing the menace of cyber-crimes.

iii. Design and development

The evaluation of some existing cybersecurity best practices, guidelines and framework's literature were used to evaluate the implementation of a cybersecurity framework. As much as the reviewed standards and frameworks are of a very good benefit to the banking industry, a lot has to be done since they have some levels of incompleteness. In addition to that, semi-structured interviews were used to assess the various patterns of cybercrimes associated with online transactions and to evaluate the existing cybersecurity frameworks in banks as this assisted the researcher in gaining an understanding of the as-is state of cyber maturity and to identify areas of improvement in the banks through designing a framework.

iv. Demonstration

To demonstrate the feasibility and efficacy of the resultant framework, a scenario of a bank was used.

v. Evaluation

The framework was evaluated by experts in the field and also those working in the banking institutions with experience in cybersecurity. The evaluation was performed with the aim of obtaining verification on the accuracy and effectiveness of the framework.

vi. Communication

The final step was to communicate the resulting framework. Also, contributions of this study were disseminated in peer-reviewed scholarly publications and also reported in a journal article.

Table 0.1 Summary of Data collection tools

Research Questions	Data Collection Tools Used
i) What are the various patterns of cybercrimes associated with online transactions in the Namibian banking institutions' cyberspace?	Semi-structured interviews
ii) What are the components/elements of existing cybersecurity frameworks and what are the missing components/elements in the Namibian context?	Literature review and semi-structured interviews
iii) How can identified elements be used to formulate a cybersecurity framework to guide the Namibian banking institutions in managing online financial transactions?	Design research methodology

5.4.1 Data Triangulation

Data collected from interviews was validated utilising triangulation. Triangulation is defined as “the use of multiple methods or data sources in qualitative research to develop a comprehensive understanding of phenomena. Triangulation also has been viewed as a

qualitative research strategy to test validity through the convergence of information from different sources” (Carter, Bryant-Lukosius, DiCenso, Blythe, & Neville, 2014, p. 545). There are various types of triangulation namely, method triangulation, investigator triangulation, theory triangulation and data source triangulation.

This study used data source triangulation, which entails gathering information from a variety of people, including individuals, organisations, families, and communities, in order to obtain diverse views and data validation (Carter et al., 2014). To improve the credibility and internal validity of the research findings, triangulation was applied (Merriam & Tisdell, 2016). The researcher used various data sources to confirm the emerging findings. The researcher triangulated the various data sources by comparing and cross-checking data collected through the interview from correspondents with different perspectives with the same correspondents. In this way, the researcher had thus employed triangulation by using two methods; semi-structured interviews and bank records.

Triangulation methodology assisted in confirming research findings, as data was more comprehensive, and there were increased validity and improved understanding of the topics explored (Bekhet & Zauszniewski, 2012). The study thus triangulated data from two data sources, namely semi-structured interviews and reports from local banks. This was done to assess the various patterns of cybercrimes associated with online transactions and evaluate the existing cybersecurity frameworks as this assisted the researcher in gaining an understanding of the as-is state of cyber maturity and identify areas of improvement in the banks through designing a framework. Triangulation was used to promote the validity and dependability of data.

3.5 Research Population

A research population is defined as the actual segment of reality the researcher would like to study (Verschuren, Doorewaard, & Mellion, 2010). The population used for this study

consisted of staff from 6 out of 10 licenced banks in Namibia. This included, six commercial banking institutions in Namibia, namely Bank BIC Namibia Limited, Bank Windhoek Namibia Limited, First National Bank Namibia Limited, Nedbank Namibia Limited, Letshego Bank Namibia Limited (micro-finance banking institution) and Trustco Bank Namibia Limited.

3.6 Sample and Sampling Technique

Since it is not feasible to study the entire population in the chosen banks, a sample was selected to participate in the study. The study, therefore, adopted a purposive sampling method to determine the study sample. Purposive sampling, “is typically used in qualitative research to identify and select the information-rich cases for the most proper utilisation of available resources” (Etikan, Musa, & Alkassim, 2016, p.2). In this case, individuals that had well informed knowledge and experience about cybersecurity were identified and selected.

With the use of purposive sampling procedure, a sample of 1-2 out of the total number of employees within IT departments were selected. The sample was selected according to the well-known IT positions in the Namibian companies, namely Information security manager, Information security specialist, network engineer, IT risk analysts and system administrators. The selected sample was believed to have in-depth knowledge of cybersecurity threats and incidences.

According to Gray (2014), “stratified random sampling is a method for achieving a greater degree of representativeness and for reducing the degree of sampling error” (p. 210). Stratified sampling technique was therefore applied in this study. The sample was divided into various sub-groups known as “strata”, sharing common characteristics such as experience and responsibilities. A sample was taken from each stratum to ensure representation of all the groups in the needed population (Acharya, Prakash, Saxena, & Nigam, 2013).

To obtain interesting events pertaining to cybersecurity in the banks, the best people interviewed were a stratum of the experts and knowledgeable staff in the IT field, which are the IT staff such as Information security manager, Information security specialist, network engineer, IT risk analysts and system administrators. The total sample size was 8 which is believed to be the saturation point as no new insights could be gathered.

Table 3.2 summarises the population size of the study.

Table 0.2 Population sample

Population	Sample
Number of selected banks	6
Total number of selected staff per bank	1-2
Total sample size	8

3.7 Data Analysis for Qualitative Research

Data analysis is the process of condensing, summarising, grouping/categorising and reorganising non-standardised and complex acquired data into usable information (Saunders et al., n.d.). There are two approaches in qualitative data analysis, namely the deductive approach and inductive approach (Gray, 2014).

Firstly, the deductive approach is one in which the researcher develops a theory and hypothesis before devising a research technique to evaluate the theory (Saunders et al., n.d.). The researcher normally starts with a theory that they find convincing and use a broad level to a more specific one. A deductive research method is associated with positivism research paradigm. The researcher tests hypotheses that emerge from theories of studies that have been completed by others (Saunders et al., n.d.).

Secondly, the inductive approach is the approach whereby the researcher collects data with the aim to develop a theory (Saunders et al., n.d.). Inductive research does not require the creation of a hypothesis. Inductive techniques aid in grasping meaning in complex data by

creating a summary of themes or categories from the raw data, a process known as data reduction. An inductive research approach is typically associated with interpretivism research paradigm.

This study was informed by the use of inductive research design. Saunders et al. (2016) state that the inductive approach allows the researcher to have explanations on what is going on and understand why something is happening. This research process was all about assessing the various patterns of cybercrimes associated with online transactions and evaluating the existing cybersecurity frameworks in an attempt to assist the researcher in gaining an understanding of the as-is state of cyber maturity and identify areas of improvement in the banks through designing a framework. Gray (2014) states that qualitative research are frequently connected with inductive research designs whereby numerous techniques and approaches are utilised for collecting data from diverse standpoints.

According to Wagner et al. (2012, p. 10), “one of the main sources of data analysis is audiotapes and/or videotapes which will be taken from discussions of the group interviews”. A detailed, verbal description of the characteristics informed by the semi-structured interviews was used for this qualitative research. Each interview was transcribed from the audio recording. Editing was thus performed to improve the readability of the transcript after the transcription process as there was a need to edit and ensure that meaning is preserved.

For this study, audio recordings of interviews were therefore used for data analysis. According to Wagner, Kawulich, and Garner (2012), when constructing and analysing data, respondents settings and nonverbal communication are crucial input. Content analysis is one of the most frequent methods used for analysing qualitative data. “Essentially, this involves the making of inferences about data (usually text) by systematically and objectively identifying special characteristics (classes or categories) within them” (Gray, 2014, p. 607).

The transcript was analysed qualitatively by identifying major substantive points which were then grouped into themes and categories. Content analysis was used to classify numerous words of the text into a smaller number of content categories. The content categories were then used as components to develop the cybersecurity framework.

3.8 Data Analysis Plan

After data had been collected from a sampled population, the next step was to analyse the data to answer research questions. Data analysis is the process of condensing, summarising, grouping and categorising non-standardised and complex collected data to become meaningful information (Lewis, Thornhill, & Saunders, 2016).

Although most of the data were analysed via description, the researcher went beyond description by interpreting, understanding and explaining the data. New insight into data was therefore gained through this analysis. According to De Hoyos and Barnes (2012), qualitative data analysis entails the processes of identifying and organizing, coding, conceptualising and categorising themes found in the data to provide meaning.

Figure 3.2 presents the qualitative analysis process by Merriam and Tisdell (2016).

Qualitative analysis process

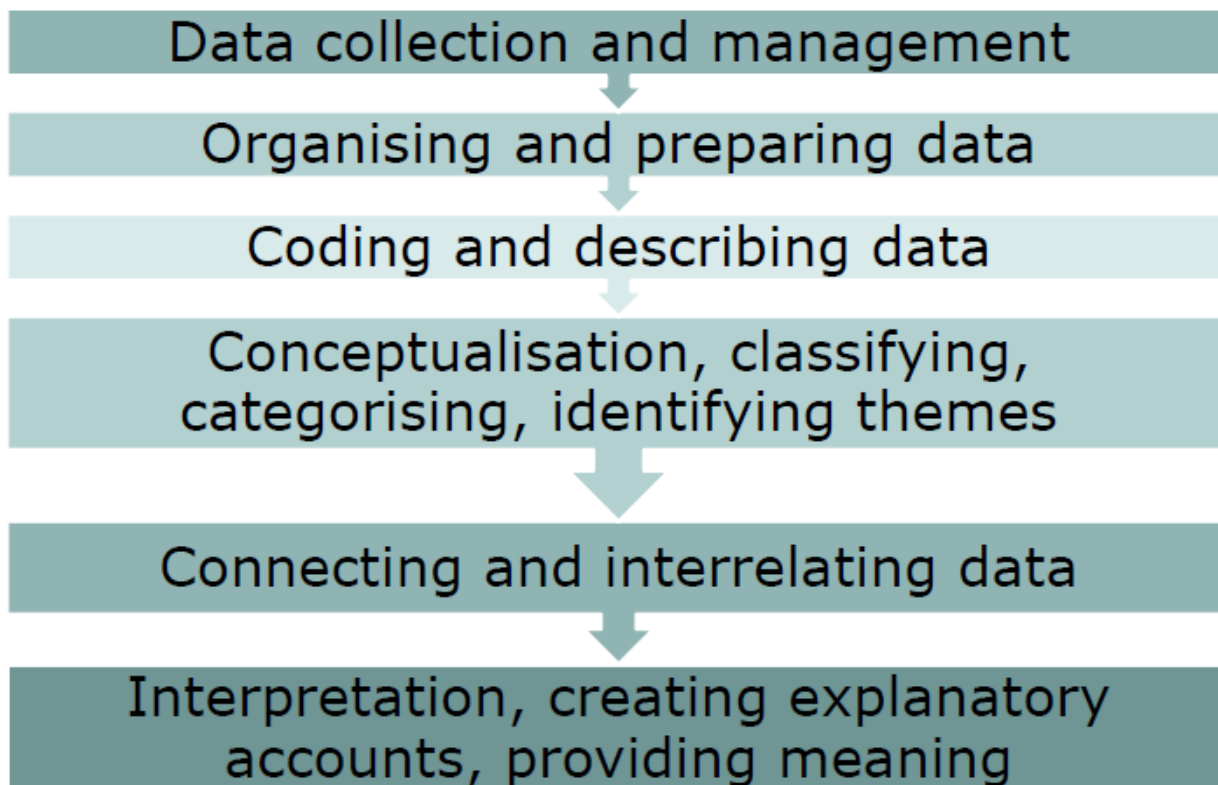


Figure 0.2 Qualitative analysis process

The data analysis plan adopted in this research followed six sub-processes (refer to the processes described in details sections 3.8.1 through 3.8.6).

3.8.1 Data Collection and Management

Data collected via interviews were recorded and then analysed through a technique known as coding. Coding is the process of converting raw data into a uniform format for data analysis (Merriam & Tisdell, 2016). The results of data coding are commonly called categories or themes as they are answers to the research questions, and it is the research questions that guide the analysis and coding of the raw data.

3.8.2 Organising and Preparing Data

This was achieved through content analysis as the researcher explored the insights and beliefs that emerged from the data. This allowed the researcher to develop categories or themes from the data. The researcher repeatedly listened to the interview audio recordings and transcribed the interview content onto the word document. Key points in the transcript were identified then grouped into themes and categories. Subsequently, the transcribed text was then validated against the audio recordings to ensure that the data was accurate.

Table 3.3 provides a sample of the semi-structured interview questions.

Table 0.3 Sample of the semi-structured interview questions

Respondents	Interview Question
	1. What are the national and local standards that your organisation complies to?
	2. Have you adopted any cybersecurity standard/framework, how have you adjusted it to fit the enterprise needs?
	3. Do you have any formal documented policies, procedures, and key documents in regards to information/cyber security, allowing stakeholders to get all the needed information?
	4. What are the various types of cybercrimes associated with online transactions have you experienced in your organisation?
	5. Does your organisation have a security program?
	6. Has your organisation experienced any cyber-attack over the past 2 years?
	7. What do you think is the main vulnerability for cyber-attacks in your organisation?
	8. Do you have an incident handling process in place, is it adhered to by all stakeholders?
	9. Is the top management involved in driving the information security of the bank? How?
	10. How does your bank identify, protect, detect, respond and recover from cyber events?
	11. Do you offer any of your stakeholder's cybersecurity training?

3.8.3 Coding and Describing Data

After themes were identified within the text, the next step was the analysis - data coding process. Codes were grouped by commonality to create categories and finally themes. The coded text was

then manually sorted to analyse the patterns found. The final stage involved establishing common themes, which in turn generated a concept which was represented in the form of a conceptual framework.

3.8.4 Conceptualisation, Classifying, Categorising, Identifying Themes

After the transcription process, the researcher manually identified themes and categories which were used in referencing the data.

3.8.5 Connecting and Interrelating Data

Interview data were interrelated and identified themes and categories were summarised into research findings.

3.8.6 Interpretation, Creating Explanatory Accounts, Providing Meaning

In the end, the research findings were analysed and interpreted into meaningful context which informed the design of the framework.

Table 3.4 links research objectives to the research methodology as articulated in section 3.3 through 3.8:

Table 0.4 research objectives vs research methodology

Objective	Research Question	Methods/tools/strategies
Assess the various patterns of cybercrimes associated with online transactions in the Namibian financial institutions' cyberspace	What are the various patterns of cybercrimes associated with online transactions in the Namibian financial institutions' cyberspace?	Methods: Qualitative Tools: secondary data analysis and semi-structured Interviews Strategy: qualitative exploration approach
Evaluate existing cybersecurity frameworks	What are the components/elements of existing cybersecurity frameworks and what are the missing components/elements in the Namibian context?	Methods: Qualitative Tools: Literature review and semi-structured interviews Strategy: qualitative exploration approach
Develop a cybersecurity framework to guide Namibian banking institutions in managing online financial transactions	How can identified elements be used to formulate a cybersecurity framework to guide the Namibian financial institutions in managing online financial transactions?	Methods: Qualitative Tools: Design research methodology Strategy: qualitative exploration approach

3.9 Research Methodology Limitations

Responses were limited to participants' willingness to provide real scenario cases and also to disclose their internal incidences on cybersecurity as fear of losing their brand reputation.

3.10 Assumptions

For this research, the following assumptions were considered:

- i. The assumption was that the sampled banks would support this research by providing all the necessary information requested by the researcher.
- ii. The selected banks would be interested in the adoption of the cybersecurity framework.

3.11 Ethical Considerations

Ethical considerations across the research community are critical due to issues related to legislation regarding human rights and privacy concerns. Ethics refer to principles of right and wrong that guide research conduct (Muganda, 2010). Even if not explicitly specified, researchers are expected to be aware of and abide by what is regarded as acceptable ethical conduct.

This study, therefore, abided to some of the universally accepted ethical standards, which include obtaining informed consent from all participants. Besides, it included issues such as voluntary participation, anonymity and confidentiality - the principle of assuring that the interests, well-being and identity of research participants were protected. Since some of the data might be sensitive, the researcher made it clear that no confidential or sensitive information would be revealed, unless prior permission is obtained. Lastly, an ethical clearance was obtained from the faculty.

3.12 Chapter Summary

This chapter conferred the research methodology. This study used an interpretive research paradigm and a qualitative research approach to test the assumptions of the banks about cybersecurity. An interpretive approach employed the triangulation strategy to ensure validity and reliability. A purposive sampling technique was applied to determine the study sample because it selects information-rich cases. Data were collected using semi-structured interviews and discussions with staff from different commercial banks to obtain qualitative data. Each interview was transcribed from the audio recording and a qualitative content analysis was performed of which data were grouped into themes and categories.

CHAPTER FOUR: DATA ANALYSIS

4.1 Overview

Data analysis is the process of condensing, summarising, grouping and categorising non-standardised and complex collected data to become meaningful information (Lewis, Thornhill, & Saunders, 2016). After data had been collected from a representative sample in the population, the next step was to analyse the data to answer the following research questions: (i) what are the various patterns of cybercrimes associated with online transactions in the Namibian financial institutions' cyberspace? (ii) what are the components/elements of existing cybersecurity frameworks and what are the missing components/elements in the Namibian context?

This chapter presents a detailed semi-structured interviews data analysis. Also, coding and transcription of collected data are discussed where themes and categories are identified from the collected data. A discussion of and presentation of research findings in relation to the research objectives are also presented.

4.2 Analysis of Data

The data analysis plan presented in section 3.8 was applied to the collected data following six sub-processes as presented in section 4.2.1 through 4.2.6.

4.2.1 Data Collection Management

Data collected via interviews were recorded and then transcribed. The data were further analysed through a technique known as coding. The research questions guided the analysis and coding of the raw data.

4.2.2 Organising and Preparing Data

This was attained by repetitively listening to the audio recordings of the semi-structured interviews and transcribing the interviews on to a word document. Subsequently, the

transcribed text was then verified against the audio recordings for accuracy and completeness of the text. Data were transcribed and presented in table 4.1.

B stands for bank and R stands for respondent

Table 4.1 Organised semi-structured interview questions

Respondent	1. Did your organisation experience any cyber-attacks over the past years?
B1R1	<i>Yes</i>
B2R1	<i>Yes</i>
B2R2	<i>Yes</i>
B3R1	<i>Yes, the bank is always under attack</i>
B4R1	<i>Yes, everyday</i>
B5R1	<i>No, however there has been cases when we have upgraded systems and had downtimes but not attacks.</i>
B6R1	<i>Yes</i>
B6R2	<i>Yes</i>
	2. What were the various types of cyber-attacks experienced? How many of the attacks were successful and managed to compromise the environment?
B1R1	<i>Phishing, and compromise of the bank website. The compromise of the online platform was successful as attackers managed to get access to client's VISA accounts.</i>
B2R1	<i>Phishing and social engineering, vishing, DNS-poisoning/spoofing. None of the attacks were successful.</i>
B2R2	<i>Online banking infrastructure - websites, database SQL attacks and vulnerability against web resources such as websites and SharePoint. None of the attacks were successful as the bank has a multi-layer firewall environment.</i>
B3R1	<i>Phishing attacks – clients being targeted and spear phishing attacks to employees. None of them have compromised the environment.</i>
B4R1	<i>Phishing attacks, malware and botnets and all are mostly email oriented. The bank currently does not have an online banking system (they are not a transactional bank yet). None of the attacks were successful.</i>
B5R1	<i>Fraudulent actors would be compromised through clients and not necessarily an attack of the banking services, platforms and systems. None of the attacks were successful.</i>
B6R1	<i>Phishing mails, attack of the malware server and DDoS attack. The banking institutions are exposed to multiple cyber-attacks on a daily basis, where scammers attempt to hack their systems or plant viruses that impact system availability. None of the attacks were successful.</i>
B6R2	<i>Phishing attacks, vishing attacks (syndicates that call clients randomly) and card-not-present attacks (clients get SMS that money has been deducted on their accounts in other countries while they haven't travelled) which is known as smishing. None of the attacks were successful.</i>

	3. Are these types of cyber-attacks associated with online transactions?
B1R1	<i>Yes, as it was a compromise of the online platform (website) and attackers compromised the client's VISA accounts.</i>
B2R1	<i>Most of them were due to online interactions, not necessarily transactional related. The use of corporate emails to request online services as it increases the exposure of internal email addresses to public domains.</i>
B2R2	<i>Yes, as it is a compromise of the online banking platform (website).</i>
B3R1	<i>Yes, phishing attacks targeted to customers target online transactions as it is the easiest way to gain access to client information.</i>
B4R1	<i>No, the bank does not have an online banking system.</i>
B5R1	<i>No, the attacks are not directly associated with online transactions.</i>
B6R1	<i>Yes, most of them targeted online transactions such as denial of service attacks</i>
B6R2	<i>Yes, most of them were online transactions oriented</i>
	4. What do you think is the main vulnerability for cyber-attacks experienced in your organisation?
B1R1	<i>Lack of user awareness training, loopholes and vulnerabilities in systems, lack of two-factor authentication and lack of implementation of firewall policies.</i>
B2R1	<i>People remain the weakest link in the security chain and so are the main vulnerability for most organisations. The conduct and behaviour of users in any environment plays a vital role and this includes both end users and technology users/owners. Another vulnerability is misconfigurations of systems/applications by technology owners by not prioritising the hardening of systems and applications.</i>
B2R2	<i>Websites are the main vulnerability, the way website are written and set up and only upgraded and patched in a short-time. Another vulnerability is scams with phishing and vishing. Lastly, users compared to business requirements is also a vulnerability as most of the times they completely ignore the security aspects.</i>
B3R1	<i>People are always the main vulnerability, even with appropriate awareness, people are still the weakest link as its always easy to manipulate people and they always lack judgemental skills so it is easy to compromise a person.</i>
B4R1	<i>People will always remain the weakest link. Also, not all systems have multi-layer of security and there is lack of network layer firewall.</i>
B5R1	<i>The biggest vulnerability is the ability to apply basic information security practices and implement basic principles, procedures and basic standards. Organisations should at least have sort of basic information security practices being applied although not across all platforms. Namibia however did not have the best internet connectivity hence why there hasn't been successful attacks.</i>
B6R1	<i>Bugs in operating systems where hackers are exploiting the vulnerabilities and lack of employees awareness - employees failing to understand cyber security risk is also a great risk as employees will always be the weakest link</i>
B6R2	<i>Phishing emails that goes around the organisation and people as they remain the weakest link.</i>
	5. How did you handle/contain the types of cyber events mentioned above?
B1R1	<i>Reviewed the security infrastructure and integrated the two-factor authentication such as biometric, password encryption, PINs, SMS and email notifications.</i>

B2R1	<i>By blocking the suspicious addresses that aimed to have access to the environment and where applicable blocking or rerouting traffic of attackers. Another key area was awareness and notification to affected users and the entire organisation to be reminded of the precautions and immediate incidents reporting.</i>
B2R2	<i>The bank has a multi-layer firewall infrastructure, regular review of attacks to identify the patterns of the attacks and then adjust the firewall rules. The network engineers also distinguish between attacks and vulnerabilities and vulnerabilities are analysed at least once a month in detail and take measures to prevent for future use.</i>
B3R1	<i>Emails have been reported and domains were blocked by network engineers. Spam filters and checkpoint systems were put in place that can reduce the number of phishing emails coming through to employees. The bank has proper channels available to report the cyber incidents, we have a proper incident management plan and procedure.</i>
B4R1	<i>Introduced multi-factor-authentication on transactions.</i>
B5R1	<i>Implemented awareness for their clients in order to implement efficiency and convenience for information security. Ensure that whatever is implemented especially online platforms have to be efficient and convenient. For their online platform they have tokens for internet banking as a way to ensure client convenience.</i>
B6R1	<i>Regular vulnerability scans on all platforms to identify vulnerabilities in operating systems, regular system security patches are also performed, also doing phishing mail campaigns for the employees.</i>
B6R2	<i>There are Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) which blocks all communications from Russia to graphical areas as the bank does not have clients there as well as firewalls. There are also formal training and awareness in place, the bank also offer awareness to clients on public platforms such as websites and newspapers and also send private awareness emails to clients to make them aware.</i>
	6. Are your organisation's personnel properly trained and understand the nature of cyber security and their role in protecting the organisation's information asset?
B1R1	<i>IT Personnel are fully trained on recent cyber-attacks and the bank has a certified ethical hacker based in Portugal (head office). All staff are forced to attend induction training which also involve IT components but not specifically on information security or cyber security.</i>
B2R1	<i>They are partially trained, however due to high number of staff in remote areas, it has been a challenge ensuring that all staff members are aware of the importance of cyber security and their roles in ensuring that they play their part in contributing to the security of the organisation. The bank has invested in an awareness solution that will eliminate the distance and remote limitation of accessing users in the various locations/sites. The solution will be rolled out as a web based solution that will assign users awareness trainings on all critical topics of cybersecurity, simulations and assessments to measure the effectiveness of the trainings issued per user and as an overall organisation.</i>
B2R2	<i>Try to train as cybersecurity is a multidisciplinary art, so it is difficult to train users with detailed training. It is better if the team has specialised people in an existing IT field as cybersecurity because in order to prevent attacks one needs to have a deeper understanding of the infrastructure, communications between systems and it is difficult to gain. Reviewing of logs helps identify patterns, cybersecurity has no mandate and roles to focus solely on cybersecurity. Information security is a policy maker and a policy maker cannot be a policy implementer, hence why cybersecurity personnel has to be independent.</i>

B3R1	<i>They are not fully trained as more training is currently being rolled out on cybersecurity through security awareness platforms. The training is aimed to track performance and test staff understanding of cybersecurity. We are not where we are supposed to be yet.</i>
B4R1	<i>No, they are not properly trained. Although the bank does targeted phishing simulations, employees are aware of the risks involved but do not understand and know how to protect the organisation.</i>
B5R1	<i>Quite low in maturity as we have only recently acquired a learning management platform. Information classification framework is yet to be embedded in the process. Ad-hoc awareness is done via email and posters, PC login prompts, policies have been put in place to enhance the security culture such as not allowing shoulder surfing. The organisation had also introduced single sign on (SSO).</i>
B6R1	<i>Employees are fairly trained although cybersecurity attacks do change constantly as hackers always try to find new vulnerabilities and new ways of compromising organisations. The aim is therefore to constantly keep on training the employees</i>
B6R2	<i>Yes, employees are partially trained through formal training, although training awareness is not fully in place as the bank recently deployed a training platform to address cybersecurity awareness. However, there is 100% commitment to start and implement the formal trainings.</i>
	7. What are the local and international information/cybersecurity standards and frameworks have you adopted in your organisation?
B1R1	<i>AML regulations and BoN FIC laws</i>
B2R1	<i>ISO27001/2, CIS, NIST, PCI-DSS, General Data Protection Regulation (GDPR), BoN BID-30</i>
B2R2	<i>PCI-DSS, BoN BID-30</i>
B3R1	<i>Not completely but there are standards we use such as PCI-DSS as we have to comply to them because it is a requirement for the industry. International and more general we cannot implement the whole framework but the appropriate controls and sections that apply to us we apply, such as ISO27001/2, CIS, BoN BID-30.</i>
B4R1	<i>None, the bank only has operational driven procedures that follow COBIT and Information Technology Infrastructure Library (ITIL) guidelines.</i>
B5R1	<i>ISO, CIS, NIST, PCI-DSS, COBIT, ITIL, BoN BID-30.</i>
B6R1	<i>PCI-DSS and ISO27001 and ISO27002</i>
B6R2	<i>PCI-DSS and ISO27001/ ISO27002 and NIST</i>
	8. Have you fully adopted each standard/framework's functions, categories and/or elements?
B1R1	<i>No</i>
B2R1	<i>Yes, the ISO27001/2 and PCI-DSS, however as for NIST, GDPR, BoN BID-30 and CIS only some elements are adopted.</i>
B2R2	<i>Organisational functions are not clearly defined as the standards propose, or as per best practice and there is no dedicated cybersecurity team that is in the disciplinary of cybersecurity as the team is a network team.</i>
B3R1	<i>Not fully adopted the frameworks. It is impossible to conform to all frameworks and standards, especially because companies are different and have different requirements. A good way of doing</i>

	<i>it is see what most of them have in common, like sections and try and implement that in our environment.</i>
B4R1	N/A
B5R1	<i>We try and take elements from the frameworks and embed them within our own set of framework and apply them internally. We do not blanketly apply the frameworks as they are as we might be detrimental to the organisation as we end up spending too much or less on the controls or doing things we must not be doing.</i>
B6R1	<i>For PCI-DSS we have fully adapted the standard as-is because all banking institutions have to comply to it. As for ISO27001 and ISO27002 only few elements were adapted in the organisation's frameworks and standards as not all of them are applicable in our environment.</i>
B6R2	<i>Not fully apart from PCI-DSS as the bank has to comply to the standards. For others, the bank only adapt the elements and controls that are applicable and that can be implemented.</i>
	9. Do you think there are some important aspects and elements that the international standards and frameworks did not cover? What are those elements and why do you believe they were supposed to be part of the standards/framework?
B1R1	<i>Most of them overlap as they are more on financial regulations.</i>
B2R1	<i>Data protection and privacy, although some standards cover data classification for the purpose of access list. The handling of sensitive data is fully enforced by most of the standards.</i>
B2R2	<i>PCI-DSS is a more technology based standard and the human factor such as soft skills are missing; they are either weak or not emphasized. Although they state it's not their focus.</i> <i>Principle of Least Privilege (POLP), and public knowledge on information security practices is also not well defined, different roles within teams are not well defined e.g. what the systems engineers and network engineers need to know and what they do not need to know.</i> <i>Aspect of disaster recovery documentation is also missing, how is it documented and what needs to be documented. If you have a proper documentation, for example, will be a master key to the firewall environment. It is very critical in terms of cybersecurity attacks that the documentation of a disaster recovery forms the ability to recover from a disaster, cannot design a framework without guidance on how to recover from an incident because a framework should say, if you follow this you will never have a cyber-attack hence a guideline on how to recover from an attack should be part of the documentation.</i>
B3R1	<i>Yes, they do cover everything, 99% of them cover, but you have to search across them to search the controls you are looking for. But individually they do not cover all aspects as they lack a lot of things in different areas. The main important thing when using these standards is what is the target audience as it matters most. Something that is rarely mentioned in this frameworks is people because you can rarely put a control on a person, they touch everything about people but the people factor is missing in most of them.</i>
B4R1	<i>N/A. The bank currently does not have a cybersecurity team and only has recently appointed an Information Security Specialist.</i>
B5R1	<i>Everything is covered as most of them detail what you need to be doing even to a granular level. Some of them are more detailed or have more perspective but I cannot think of any factor that is not covered at all.</i>
B6R1	<i>Yes, for example ISO27001 and ISO27002 they lack cyber breach simulations as this will give them a better understanding of how to contain the incident in case of a breach.</i>

B6R2	<i>Not really, as everything in the standards is relevant. There are also industry updates every year of which standards get updated and aligned to the latest best practices. The only gap is that there is lack of awareness on these standards in organisations.</i>
	10. What value would these elements add to the standard/framework?
B1R1	<i>None that they are aware of.</i>
B2R1	<i>Seeing that information is the most valuable asset within the cyber chain as without it nothing much can be done by the attackers. The element of privacy would ensure data users and data handlers both take precautions before providing and processing of any type of information.</i>
B2R2	<i>This will help in having an effective and holistic cybersecurity program. The European Union cybersecurity response team/agency is busy with CISO teams which will have specific frameworks.</i>
B3R1	<i>Since the weakest link is people , adding the people factor to the frameworks will help to mitigate the biggest risk of human factor but if there is constant awareness, you change the culture and there will be less issues.</i>
B4R1	<i>N/A</i>
B5R1	<i>Organisations just need to try and identify the elements that are key for their environment and try and embed them in their organisation.</i>
B6R1	<i>Once the standard include the cyber breach simulations, organisations will be able to know what to do during a cyber-incident.</i>
B6R2	<i>N/A as all standards cover all the important aspects of information security.</i>
	11. Do you have any policies, procedures and programs that support the information security function which helps the function in identifying cyber security risks, strengths, and weaknesses?
B1R1	<i>IT policies such as user logging, firewall policy and anti-malware and deletion policy.</i>
B2R1	<i>IT Risk framework that highlights the key areas of concerns. It also classifies cybersecurity as a level 2 risk. Security automated vulnerability scans (Nexpose), penetration tests (Sysnet), anti-malware software report statistics guard the directions.</i>
B2R2	<i>Yes, the bank has information security policies and incident management plans. The system architect team reports cybersecurity risks and not the Information Security Manger(ISM).</i>
B3R1	<i>There is an acceptable use policy which covers how devices are used, information security policy which states what information needs to be secured and understand what you are working with and how to protect it. The Information Security policy clearly stipulates cybersecurity as a risk and there are controls in place to mitigate the risk.</i>
B4R1	<i>The bank has one IT policy only which covers everything in IT.</i>
B5R1	<i>We have a number of documented procedure but with all the policies we have tried to put KRIs in place and try and put controls and put actions in place to mitigate the risks.</i>
B6R1	<i>There is an information security policy which is used for guidelines in the organisation.</i>
B6R2	<i>An Acceptable use policy and cybersecurity manual which is currently in a draft format and will be implemented this year.</i>

4.2.3 Coding and Describing Data

After having identified categories within the text, through the use of a word document, the researcher manually identified concepts that were used in referencing the data. The word document was used to manually highlight the identified themes and categories. The next step was the analysis itself (data coding process). Codes were grouped by commonality to create categories and finally themes. The coded text was then manually sorted to analyse the patterns found. The final stage involved establishing common themes, which in turn generated a concept which was represented in the form of a conceptual framework.

Table 4.2 summarises the data codes.

Table 4.2 Data Codes

Respondent	1. Did your organisation experience any cyber-attacks over the past years?
B1R1	Yes
B2R1	Yes
B2R2	Yes
B3R1	Yes, the Respondent bank is always under attack
B4R1	Yes, everyday
B5R1	No, however there has been cases when we have upgraded systems and had downtimes but not attacks.
B6R1	Yes
B6R2	Yes

A diagram consisting of a rectangular box on the right containing the word "Yes". Eight blue arrows originate from the "Yes" text in the response cells of the table rows B1R1, B2R1, B2R2, B3R1, B4R1, B6R1, and B6R2, all pointing towards the central "Yes" box. The arrow from B5R1 does not point to the box.

Respondent	2. What were the various types of cyber-attacks experienced? How many of the attacks were successful and managed to compromise the environment?
B1R1	Phishing, and compromise of the bank website. The compromise of the online platform was successful as attackers managed to get access to clients' VISA accounts.
B2R1	Phishing, social engineering, vishing, DNS-poisoning/spoofing. None of the attacks were successful.
B2R2	Online banking infrastructure - websites, database-SQL attacks and vulnerability against web resources such as websites and sharepoint. None of the attacks were successful as the bank has multi-layer firewall environment.
B3R1	Phishing attacks – clients being targeted and spear phishing attacks to employees. None of them have compromised the environment.
B4R1	Phishing attacks, malware and botnets and all are mostly email oriented. The bank currently does not have an online banking system (they are not a transactional bank yet). None of the attacks were successful.
B5R1	Fraudulent actors would be compromised through clients and not necessarily an attack of the banking services, platforms and systems.
B6R1	Phishing mails, attack of the malware server and DDoS attack. None of the attacks were successful. The banking institutions are exposed to multiple cyber-attacks on a daily basis, where scammers attempt to hack their systems or plant viruses that impact system availability. None of the attacks were successful.
B6R2	Phishing attacks, vishing attacks (syndicates that call clients randomly) and card-not-present attacks (clients get SMS that money has been deducted on their accounts in other countries while they haven't travelled) which is known as smishing. None of the attacks were successful.

Phishing &
Vishing, spear
phishing attacks
attacks

Online platform,
websites

Respondent	3. Are these types of cyber-attacks associated with online transactions?
B1R1	<i>Yes, as it was a compromise of the online platform (website) and attackers compromised the client's VISA accounts.</i>
B2R1	<i>Most of them were due to online interactions, not necessarily transactional related. The use of corporate emails to request online services as it increases the exposure of internal email addresses to public domains.</i>
B2R2	<i>Yes, as it is a compromise of the online banking platform (website).</i>
B3R1	<i>Yes, phishing attacks targeted to customers target online transactions as it is the easiest way to gain access to client information.</i>
B4R1	<i>No, the bank does not have an online banking system.</i>
B5R1	<i>No, the attacks are not directly associated with online transactions.</i>
B6R1	<i>Yes, most of them targeted online transactions such as denial of service attacks.</i>
B6R2	<i>Yes, most of them were online transactions oriented.</i>

Online platform &
Online transactions

Respondent	4. What do you think is the main vulnerability for cyber-attacks experienced in your organisation?
B1R1	<i>Lack of user awareness training, loopholes and vulnerabilities in systems, lack of two-factor authentication and lack of implementation of firewall policies.</i>
B2R1	<i>People remain the weakest link in the security chain and so are the main vulnerability for most organisations. The conduct and behaviour of users in any environment plays a vital role and this includes both end users and technology users/owners. Another vulnerability is misconfigurations of systems/applications by technology owners by not prioritising the hardening of systems and applications.</i>
B2R2	<i>Websites are the main vulnerability, the way website are written and set up and only upgraded and patched in a short-time. Another vulnerability is scams with phishing and vishing. Lastly, users compared to business requirements is also a vulnerability as most of the times they completely ignore the security aspects.</i>
B3R1	<i>People are always the main vulnerability, even with appropriate awareness, people are still the weakest link as its always easy to manipulate people and they always lack judgemental skills so it is easy to compromise a person.</i>
B4R1	<i>People will always remain the weakest link. Also, not all systems have multi-layer of security and there is lack of network layer firewall.</i>
B5R1	<i>The biggest vulnerability is the ability to apply basic information security practices and implement basic principles, procedures and basic standards. Organisations should at least have sort of basic information security practices being applied although not across all platforms. Namibia however did not have the best internet connectivity hence why there hasn't been successful attacks.</i>
B6R1	<i>Bugs in operating systems where hackers are exploiting the vulnerabilities and lack of employees awareness - employees failing to understand cyber security risk is also a great risk as employees will always be the weakest link</i>
B6R2	<i>Phishing emails that goes around the organisation and people as they remain the weakest link.</i>

user awareness training, misconfigurations of systems, two-factor authentication, firewall policies.

People, phishing and vishing scams, spear phishing attacks

Respondent	5. How did you handle/contain the types of cyber events mentioned above?
B1R1	Reviewed the security infrastructure and integrated the two-factor authentication such as biometric, password encryption, PINs, SMS and email notifications .
B2R1	By blocking the suspicious addresses that aimed to have access to the environment and where applicable blocking or rerouting traffic of attackers. Another key area was awareness and notification to affected users and the entire organisation to be reminded of the precautions and immediate incidents reporting .
B2R2	The bank has a multi-layer firewall infrastructure , regular review of attacks to identify the patterns of the attacks and then adjust the firewall rules. The network engineers also distinguish between attacks and vulnerabilities and vulnerabilities are analysed at least once a month in detail and take measures to prevent for future use.
B3R1	Emails have been reported and domains were blocked by network engineers. Spam filters and checkpoint systems were put in place that can reduce the number of phishing emails coming through to employees. The bank has proper channels available to report the cyber incidents, we have a proper incident management plan and procedure .
B4R1	Introduced multi-factor-authentication on transactions.
B5R1	Implemented awareness for their clients in order to implement efficiency and convenience for information security. Ensure that whatever is implemented especially online platforms have to be efficient and convenient. For their online platform they have tokens for internet banking as a way to ensure client convenience.
B6R1	Regular vulnerability scans on all platforms to identify vulnerabilities in operating systems, regular system security patches are also performed, also doing phishing mail campaigns for the employees.
B6R2	There are Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) which blocks all communications from Russia to graphical areas as the bank does not have clients there as well as firewalls. There are also formal training and awareness in place, the bank also offer awareness to clients on public platforms such as websites and newspapers and also send private awareness emails to clients to make them aware.

Two-factor authentication, multi-layer firewall infrastructure, review attacks patterns and spam filters, regular vulnerability scans

regular system security patches, phishing mail campaigns for the employees, IDS/IPS and user training and awareness and incident plans.

Res Pond ent	6. Are your organisation's personnel properly trained and understand the nature of cyber security and their role in protecting the organisation's information asset?
B1R1	<i>IT Personnel are fully trained on recent cyber-attacks and the bank has a certified ethical hacker based in Portugal (head office). All staff are forced to attend induction training which also involve IT components but not specifically on information security or cyber security.</i>
B2R1	<i>They are partially trained, however due to high number of staff in remote areas, it has been a challenge ensuring that all staff members are aware of the importance of cyber security and their roles in ensuring that they play their part in contributing to the security of the organisation. The bank has invested in an awareness solution that will eliminate the distance and remote limitation of accessing users in the various locations/sites. The solution will be rolled out as a web based solution that will assign users awareness trainings on all critical topics of cybersecurity, simulations and assessments to measure the effectiveness of the trainings issued per user and as an overall organisation.</i>
B2R2	<i>Try to train as cybersecurity is a multidisciplinary art, so it is difficult to train users with detailed training. It is better if the team has specialised people in an existing IT field as cybersecurity because in order to prevent attacks one needs to have a deeper understanding of the infrastructure, communications between systems and it is difficult to gain. Reviewing of logs helps identify patterns, cybersecurity has no mandate and roles to focus solely on cybersecurity. Information security is a policy maker and a policy maker cannot be a policy implementer, hence why cybersecurity personnel has to be independent.</i>
B3R1	<i>They are not fully trained as more training is currently being rolled out on cybersecurity through security awareness platforms. The training is aimed to track performance and test staff understanding of cybersecurity. We are not where we are supposed to be yet.</i>
B4R1	<i>No, they are not properly trained. Although the bank does targeted phishing simulations, employees are aware of the risks involved but do not understand and know how to protect the organisation.</i>
B5R1	<i>Quite low in maturity as we have only recently acquired a learning management platform. Information classification framework is yet to be embedded in the process. Ad-hoc awareness is done via email and posters, PC login prompts, policies have been put in place to enhance the security culture such as not allowing shoulder surfing. The organisation had also introduced single sign on (SSO).</i>
B6R1	<i>Employees are fairly trained although cybersecurity attacks do change constantly as hackers always try to find new vulnerabilities and new ways of compromising organisations. The aim is therefore to constantly keep on training the employees</i>
B6R2	<i>Yes, employees are partially trained through formal training, although training awareness is not fully in place as the bank recently deployed a training platform to address cybersecurity awareness. However, there is 100% commitment to start and implement the formal trainings.</i>

Lack of information security training

Respondent	7. What are the local and international information/cybersecurity standards and frameworks have you adopted in your organisation?
B1R1	AML regulations and BoN FIC laws
B2R1	ISO27001/2, CIS, NIST, PCI-DSS, GDPR, BoN BID-30
B2R2	PCI-DSS, BoN BID-30
B3R1	Not completely but there are standards we use such as PCI-DSS as we have to comply to them because it is a requirement for the industry. International and more general we cannot implement the whole framework but the appropriate controls and sections that apply to us we apply, such as ISO27001/2, CIS, BoN BID-30.
B4R1	None, the bank only has operational driven procedures that follow COBIT and ITIL guidelines.
B5R1	ISO, CIS, NIST, PCI-DSS, COBIT, ITIL, BoN BID-30.
B6R1	PCI-DSS and ISO27001 and ISO27002
B6R2	PCI-DSS and ISO27001/ ISO27002 and NIST

ISO27001 and
ISO27002, CIS, NIST,
PCI-DSS, GDPR, BoN
BID-30, COBIT and
ITIL

Respondent	8. Have you fully adopted each standard/framework's functions, categories and/or elements?
B1R1	No
B2R1	Yes, the ISO27001/2 and PCI-DSS, however as for NIST, GDPR, BoN BID-30 and CIS only some elements are adopted.
B2R2	Organisational functions are not clearly defined as the standards propose, or as per best practice and there is no dedicated cybersecurity team that is in the disciplinary of cybersecurity as the team is a network team.
B3R1	Not fully adopted the frameworks. It is impossible to conform to all frameworks and standards, especially because companies are different and have different requirements. A good way of doing it is see what most of them have in common, like sections and try and implement that in our environment.
B4R1	N/A
B5R1	We try and take elements from the frameworks and embed them within our own set of framework and apply them internally. We do not blanketly apply the frameworks as they are as we might be detrimental to the organisation as we end up spending too much or less on the controls or doing things we must not be doing.
B6R1	For PCI-DSS we have fully adapted the standard as-is because all banking institutions have to comply to it. As for ISO27001 and ISO27002 only few elements were adapted in the organisation's frameworks and standards as not all of them are applicable in our environment.
B6R2	Not fully apart from PCI-DSS as the bank has to comply to the standards. For others, the bank only adapt the elements and controls that are applicable and that can be implemented.

Not fully adopted the frameworks only some elements are adopted

Res Pond ent	9. Do you think there are some important aspects and elements that the international standards and frameworks did not cover? What are those elements and why do you believe they were supposed to be part of the standards/framework?
B1R1	Most of them overlap as they are more on financial regulations.
B2R1	Data protection and privacy, although some standards cover data classification for the purpose of access list. The handling of sensitive data is fully enforced by most of the standards.
B2R2	PCI-DSS is a more technology based standard and the human factor such as soft skills are missing; they are either weak or not emphasized. Although they state it's not their focus. Principle of Least Privilege (POLP) and public knowledge on information security practices is also not well defined, different roles within teams are not well defined e.g. what the systems engineers and network engineers need to know and what they do not need to know. Aspect of disaster recovery documentation is also missing, how is it documented and what needs to be documented. If you have a proper documentation, for example, will be a master key to the firewall environment. It is very critical in terms of cybersecurity attacks that the documentation of a disaster recovery forms the ability to recover from a disaster, cannot design a framework without guidance on how to recover from an incident because a framework should say, if you follow this you will never have a cyber-attack hence a guideline on how to recover from an attack should be part of the documentation.
B3R1	Yes, they do cover everything, 99% of them cover, but you have to search across them to search the controls you are looking for. But individually they do not cover all aspects as they lack a lot of things in different areas. The main important thing when using these standards is what is the target audience as it matters most. Something that is rarely mentioned in this frameworks is people because you can rarely put a control on a person, they touch everything about people but the people factor is missing in most of them.
B4R1	N/A. The bank currently does not have a cybersecurity team and only has recently appointed an Information Security Specialist.
B5R1	Everything is covered as most of them detail what you need to be doing even to a granular level. Some of them are more detailed or have more perspective but I cannot think of any factor that is not covered at all.
B6R1	Yes, for example ISO27001 and ISO27002 they lack cyber breach simulations as this will give them a better understanding of how to contain the incident in case of a breach.
B6R2	Not really, as everything in the standards is relevant. There are also industry updates every year of which standards get updated and aligned to the latest best practices. The only gap is that there is lack of awareness on these standards in organisations.

Data protection and privacy, soft skills, Principle of Least Privilege (POLP) and public knowledge on information security practices, aspect of disaster recovery documentation, cyber breach simulations

Respondent	10. What value would these elements add to the standard/framework?
B1R1	<i>None that they are aware of.</i>
B2R1	<i>Seeing that information is the most valuable asset within the cyber chain as without it nothing much can be done by the attackers. The element of privacy would ensure data users and data handlers both take precautions before providing and processing of any type of information.</i>
B2R2	<i>This will help in having an effective and holistic cybersecurity program. The European Union cybersecurity response team/agency is busy with CISO teams which will have specific frameworks.</i>
B3R1	<i>Since the weakest link is people, adding the people factor to the frameworks will help to mitigate the biggest risk of human factor but if there is constant awareness, you change the culture and there will be less issues.</i>
B4R1	<i>N/A</i>
B5R1	<i>Organisations just need to try and identify the elements that are key for their environment and try and embed them in their organisation.</i>
B6R1	<i>Once the standard include the cyber breach simulations, organisations will be able to know what to do during a cyber-incident.</i>
B6R2	<i>N/A as all standards cover all the important aspects of information security.</i>

Different elements would add different values as highlighted

Respondent	11. Do you have any policies, procedures and programs that support the information security function which helps the function in identifying cyber security risks, strengths, and weaknesses?
B1R1	<i>IT policies such as user logging, firewall policy and anti-malware and deletion policy.</i>
B2R1	<i>IT Risk framework that highlights the key areas of concerns. It also classifies cybersecurity as a level 2 risk. Security automated vulnerability scans (Nexpose), penetration tests (Sysnet), anti-malware software report statistics guard the directions.</i>
B2R2	<i>Yes, the bank has information security policies and incident management plans. The system architect team reports cybersecurity risks and not the Information Security Manger(ISM).</i>
B3R1	<i>There is an acceptable use policy which covers how devices are used, information security policy which states what information needs to be secured and understand what you are working with and how to protect it. The Information Security policy clearly stipulates cybersecurity as a risk and there are controls in place to mitigate the risk.</i>
B4R1	<i>The bank has one IT policy only which covers everything in IT.</i>
B5R1	<i>We have a number of documented procedure but with all the policies we have tried to put KRIs in place and try and put controls and put actions in place to mitigate the risks.</i>
B6R1	<i>There is an information security policy which is used for guidelines in the organisation.</i>
B6R2	<i>An Acceptable use policy and cybersecurity manual which is currently in a draft format and will be implemented this year.</i>

IT policy,
Information security policies,
Acceptable use policy

4.2.4 Conceptualisation, Classifying, Categorising and Identifying Themes

A thematic approach was employed through coding. Thematic approach is a method for grouping and classifying data into themes and categories that enables the researcher to answer the research questions (Merriam & Tisdell, 2016). The following codes were applied to the raw data to classify the findings:

Table 4.3 summarises the data themes and categories

Table 4.3 Data themes and categories

Themes and categories	Data extract
Types of cyber-attacks experienced	Phishing, social engineering, vishing, smishing, spear phishing, spoofing, website compromise, and DDoS attacks as shown in table 2.2
Main vulnerability for cyber-attacks	People remain the weakest link, phishing and vishing scams, spear phishing attacks to employees, lack of user awareness training, misconfigurations of systems, lack of two-factor authentication, no implementation of basic information security practices and lack of implementation of firewall policies
Security measures in place	Two-factor authentication, multi-layer firewall infrastructure, review of the patterns of attacks and spam filters, regular vulnerability scans, regular system security patches, phishing mail campaigns for the employees, IDS/IPS and user training and awareness
Information security awareness	Lack of information security training
Information/cybersecurity standards and frameworks adopted	ISO27001 and ISO27002, CIS, NIST, PCI-DSS, GDPR, BoN BID-30, COBIT and ITIL
Aspects and elements not covered in the standards and frameworks	Data protection and privacy, human factor such as soft skills, Principle of Least Privilege (POLP), and public knowledge on information security practices, aspect of disaster recovery documentation, cyber breach simulations

4.2.5 Connecting and Interrelating Data

Interview Findings:

- Based on the interview findings, it was found that the banking institutions are exposed to multiple cyber-attacks on a daily basis, where scammers attempt to hack their systems or plant viruses that impact system availability as presented in section 4.3.2, table 4.1. When asked on the types of cyber-attacks experienced in their banks, respondents highlighted different attacks experienced in their banks. According to respondent B1R1, by indicating “phishing, and compromise of the bank website. The compromise of the online platform was successful as attackers managed to get access to client’s VISA accounts.”. Further to that, respondent B2R1 said that “phishing and social engineering, vishing, DNS-poisoning/spoofing. None of the attacks were successful”. In addition, respondent B3R1 said “phishing attacks – clients being targeted and spear phishing attacks to employees.” Other respondents such as B6R1 and B6R2 also highlighted phishing attacks, among them vishing attacks, smishing and DDoS attacks. The various cybercrime patterns thus include phishing, vishing, smishing, spear phishing, spoofing, website compromise, and DDoS attacks as presented in section 4.3.2, table 4.1. Out of the total interviewed banks, only one bank indicated that the compromise of the online platform was successful as attackers managed to get access to clients’ VISA accounts. Most of the respondents indicated that none of the attacks were successful or have managed to compromise their environments; however, vulnerabilities and threats in their online banking platforms were noted as highlighted in table 4.1.
- During the interviews, respondents were asked what they believe is the main vulnerability for cyber-attacks experienced in their banks. According to respondent B1R1, “lack of user awareness training, loopholes and vulnerabilities in systems, lack of two-factor authentication and lack of implementation of firewall policies are the main vulnerabilities.” Respondent B2R1 said that “people remain the weakest link in the security chain and so are the main vulnerability for most organisations”. Other

respondents such as respondents B2R1, B2R2, B3R1, B4R1, B6R1 and B6R2 all concurred with respondent B2R1 as they all highlighted that among all other cyber-attack vulnerabilities, people remain the weakest link. Most of the respondents indicated that one of the main cybersecurity risk areas in the banking institutions is vulnerability to phishing and social engineering. Phishing is the act of impersonating a trustworthy individual in order to acquire access to sensitive information such as usernames, passwords, and other personal identifiers. Hackers are becoming more sophisticated in their attempts to trick users into clicking on fraudulent links or opening dangerous attachments in emails. Thus, raising security awareness is important to the safety of the banks.

- The other finding as identified by respondents B2R1, B2R2, B3R1, B4R1, B5R1, B6R1 and B6R2 was that the security awareness for the banking staff was low as most of the respondents indicated that their staff are partially trained. Others stated that not all staff members are aware of the importance of cybersecurity and their roles in ensuring that they play their part in contributing to the security of the organisation. Moreover, most respondents highlighted that their banks are in the process of acquiring and implementing awareness solutions which will be used for assigning awareness trainings to all users on cybersecurity critical topics.
- The interview results highlighted that banking institutions lack targeted information security awareness campaigns which should better suit the needs of their employees in an effort to build a stronger cybersecurity culture. Their employees serve as the first line of defence against cybersecurity attacks. The main key is therefore ensuring that employees are adequately informed about how to identify and respond to cybersecurity risks and a cybersecurity awareness training programme is one of the best ways of promoting a cybersecurity culture. The awareness training programme will create more effective and targeted training campaigns that will strengthen the banking institution's human firewall. The interview results also underlined that most users do not understand

the fundamentals of incident reporting as well as the bank's specific processes and policies. Establishing incident reporting processes helps banks in developing plans to prevent incidents from happening again.

- Respondents highlighted that the banking institutions have implemented controls to prevent these attempts, threats and vulnerabilities from materialising. To protect the information and information assets from security attacks, most banking institutions have deployed multifaceted security in depth strategies from external attacks through 2-tier firewall systems and intrusion prevention systems and updated antivirus systems in all nodes internally. The institution's mobile devices are constantly monitored to ensure that incidents are identified timeously, isolated and addressed proactively. Email scanning through email security solutions ensures that emails are scanned before reaching their servers and antivirus policies are enforced to improve the security posture of information assets.
- With regards to the local and international standards and frameworks, most respondents indicated that they have adopted different standards such as ISO27001 and ISO27002, CIS, NIST, PCI-DSS, GDPR, BoN BID-30 and COBIT. Most respondents highlighted that they do not adopt the full framework; however, they take elements from the frameworks and embed them within their own set of policies and procedures and apply them internally. Lastly, respondents indicated that there are some aspects and elements not covered in the standards and frameworks. These include aspects such as data protection and privacy, the human factor such as soft skills, Principle of Least Privilege (POLP), public knowledge on information security practices, aspects of disaster recovery documentation and cyber breach simulations.

4.2.6 Interpreting, Creating Explanatory Accounts and Providing Meaning

In summary:

- According to respondent B2R1, their bank has partially adopted some information/cybersecurity standards and frameworks and these are “ISO27001/2, CIS, NIST, PCI-DSS, GDPR and BoN BID-30”. This is also similar to what most respondents such as B2R2, B3R1, B5R1, B6R1 and B6R2 also highlighted with an addition of COBIT and ITIL. Respondents also highlighted that they do not adopt the full framework; instead, they take elements from the frameworks and embed them within their own set of policies and procedures and apply them internally.
- Respondents indicated that some important aspects and elements are not covered in the existing international standards and framework. Respondent B2R1 said that “data protection and privacy, although some standards cover data classification for the purpose of access list”. Other respondents also had their unique identified elements as respondent B2R2 stated that “Principle of Least Privilege (POLP), and public knowledge on information security practices is also not well defined, different roles within teams are not well defined e.g. what the systems engineers and network engineers need to know and what they do not need to know.” Respondent B2R2 further stated that the “aspect of disaster recovery documentation is also missing, how is it documented and what needs to be documented.” In addition, respondent B6R1 indicated that, “for example ISO27001 and ISO27002 lack cyber breach simulations as this will give them a better understanding of how to contain the incident in case of a breach.” Thus elements such as data protection and privacy; human factors such as soft skills, Principle of Least Privilege (POLP), public knowledge on information security practices; as well as aspects of disaster recovery documentation, and cyber breach simulations were identified as elements not covered in the existing standards and frameworks. This is the reason why a framework for the Namibian environment and context that can cater for the peculiar challenges

being faced is needed. This will save these financial institutions the problem of having to adapt components of numerous frameworks for their use. This will also go a long way to cover some aspects and elements not covered in the various frameworks being adapted parts.

- Furthermore, the interview results indicated that in as much as the attacks were not successful, one of the main cybersecurity risk areas in the banking institutions is vulnerability to phishing and social engineering. Thus, raising security awareness is important to the safety of the banks which will be embedded in the framework for the Namibian financial institutions.

4.3 Chapter Summary

In concluding this chapter, key gaps and suggested solutions will become the objectives of the proposed framework as informed by the interview responses. It was discovered that one of the main cybersecurity risk areas in the banking sector is vulnerability to phishing and social engineering. The study also found out that people remain the weakest link. It was further discovered that security awareness for the banking staff was rated as low, as most of the respondents indicated that their staff are partially trained, and most staff are not aware of the importance of cybersecurity. The interview results also underlined that most users do not understand the fundamentals of incident reporting. In regards to the local and international standards and frameworks such as ISO27001 and ISO27002, CIS, NIST, PCI-DSS, GDPR, BoN BID-30 and COBIT, most respondents indicated that they do not adopt full frameworks however they embed some of the elements within their own set of policies and procedures. Lastly, a number of respondents however indicated that elements such as data protection and privacy; human factors such as soft skills, Principle of Least Privilege (POLP), public knowledge on information security practices; aspect of disaster recovery documentation, and cyber breach simulations are not covered in the standards and frameworks. The results from this chapter influenced the framework's components as discussed in chapter 5.

Another area worthy of note (as indicated by the respondents) is that various financial institutions in Namibia have their different methods/techniques of guarding against cybersecurity threats. The developed framework also intends to bridge this by providing a unified technique that these institutions can adapt.

CHAPTER FIVE: FRAMEWORK DESIGN

5.1 Overview

This research framework design adopted the DSRM design steps by Peffers, Tuunanen, Rothenberger, and Chatterjee (2007). Various cybersecurity frameworks were analysed in chapter 2. The reviewed literature and the semi-structured interview results were used to inform the design of the proposed Namibia Banking Cybersecurity Framework (NBCF).

This chapter presents the framework design methodology, design and development of the framework, framework demonstration, framework evaluation and it finally communicates the proposed framework.

Figure 5.1 represents the design science research processes, stated by Peffers et al. (2007) as applied in this study.

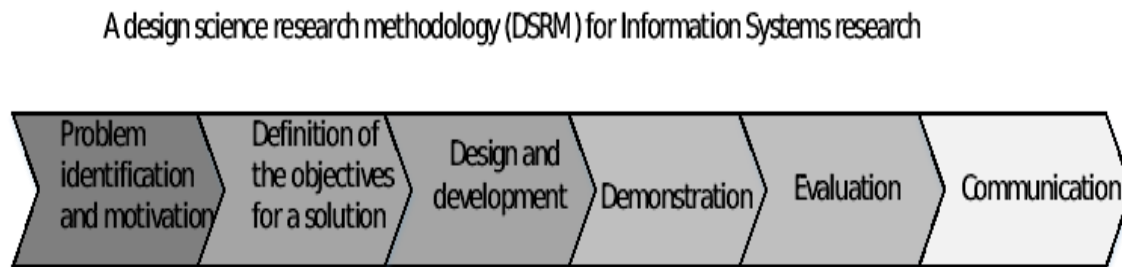


Figure 5.1 Design Science Research Methodology (DSRM)

5.2 Problem Identification and Motivation

In order to design and develop the framework, the existing cybersecurity frameworks and standards were evaluated through literature review to identify any gaps within them. In addition, semi-structured interviews conducted with bank employees also helped to identify gaps within frameworks and standards applied within the Namibian banking processes. The research identified the problem through literature reviews as lack of documented evidence of the

existence of a recognised cybersecurity framework to safeguard online transactions of financial data between banks and customers in the banking sector.

The following steps were taken in order to identify the problem:

Step 1: Analysing the current cybersecurity frameworks in Namibia

Analysis of current cybersecurity frameworks was done in chapter 2 section 2.7. The analysis concluded that cybersecurity standards and frameworks differ from country to country. This is so because of environmental and situational differences. The Namibian government is presently in the process of finalising its cybercrime related legislation which includes the draft Cybercrime Bill and the draft Data Protection Bill. Therefore, Namibia also as a sovereign nation needs to develop its framework that will be able to cater for the cybersecurity needs of both its citizens and its banking institutions.

Step 2: Global current cybersecurity attacks in the financial sector

An analysis of security challenges and corresponding types of cybersecurity attacks in the banking industry was done in chapter 2 section 2.3. Table 5.1 and table 5.2 summarises current security weaknesses and attacks in the banking industry.

Table 5.1 Security weaknesses

Current security challenges trends globally	Source
<ul style="list-style-type: none"> • Mobile and web banking security 	Yildirim and Varol, 2019
<ul style="list-style-type: none"> • The use of third parties 	Verizon, 2019
<ul style="list-style-type: none"> • Compliance issues 	Security Intelligence, 2016
<ul style="list-style-type: none"> • Insider vulnerabilities 	IBM, 2019
<ul style="list-style-type: none"> • Large user population 	IBM, 2019
<ul style="list-style-type: none"> • Gaps in technology 	ZDNet, 2018

Table 5.2 Cyber-attack types in the banking industry

Current cybersecurity attacks trends globally	Source
<ul style="list-style-type: none"> Phishing attacks 	Kaspersky Labs, 2019
<ul style="list-style-type: none"> Ransomware 	Kaspersky Labs, 2019
<ul style="list-style-type: none"> Insider Attacks 	Yaseen, 2016
<ul style="list-style-type: none"> DDoS 	Akamai, 2018

Step 3: Mapping against the cybersecurity trends

Global cybersecurity attacks in the banking sector (given in chapter 2 section 2.3) were then mapped to the Namibian context given in chapter 4 section 4.2.3 as shown in table 5.3. It was concluded that many of the global cybersecurity issues can be matched to those identified in the Namibian banks. Table 5.3 summarises these cybersecurity issues.

Table 5.3 Mapping against the cybersecurity trends

Issues Discovered	Global cybersecurity threats in the banking sector	Reference
Data protection and privacy	Mobile and web banking security The use of third parties Compliance issues Gaps in technology	Chapter 4, section 4.2.3
Human factor - soft skills	Insider vulnerabilities	Chapter 4, section 4.2.3
Principle of Least Privilege (POLP)	Large user population	Chapter 4, section 4.2.3
Public knowledge on information security practices	Large user population	Chapter 4, section 4.2.3
Aspect of disaster recovery documentation	Compliance issues	Chapter 4, section 4.2.3
Cyber breach simulations	Gaps in technology	Chapter 4, section 4.2.3
Corporate governance	Compliance issues	Chapter 2, section 2.8
Ethical conduct	Compliance issues	Chapter 2, section 2.8
Trust	The use of third parties	Chapter 2, section 2.8
Auditor security	Compliance issues	Chapter 2, section 2.8

In summary, there is an urgent need to develop a cybersecurity framework that can serve as guidance to safeguard online transactions of financial data between banks and customers. Thus, this research intends to develop a Namibia Banking Cybersecurity Framework, to assist banking institutions in safeguarding the transactions of online financial data between banks and customers. The Namibia Banking Cybersecurity Framework is a risk-based approach, assessing where cyber risks are the greatest in banks, help in identifying key critical systems, the information and data assets that require protection.

5.3 Definition of the Objectives for a Solution

To solve the problem identified in section 5.2, a Namibia Banking Cybersecurity Framework (NBCF) to guide banking institutions in safeguarding online transactions of financial data between banks and customers was developed.

The NBCF can enable the Namibian banking institutions:

- To identify critical information assets inventory and business functions,
- To detect cybersecurity attacks in the banking sector in a timely manner,
- To protect human resources and information system assets of the banking sector,
- To effectively respond to detected cybersecurity attacks,
- To recover from cybersecurity attacks, and
- To comply with organisational, national, industry, international policies, regulations and laws.

Table 5.4 summarises the Namibia Banking Cybersecurity Framework (NBCF) objectives and significance.

Table 5.4 Objectives of the NBCF and significance

Objectives of the solution	Reference to literature and data analysis	Why is it important
1. To identify critical information assets inventory and business functions	Chapter 2, section 2.7	Identifying critical information assets inventory and business functions enables banking institutions to identify risks associated with each critical asset. This will enable banking institutions to conduct comprehensive risk assessments. Hence cyber-attacks can be prevented before they occur.
2. To detect cybersecurity attacks in the banking sector in a timely manner	Chapter 2, section 2.7	Detection of attacks is of paramount importance as it helps banking institutions to respond effectively to the attacks in order to reduce the extent of the damage.
3. To protect human resources and information system assets of the banking sector	Chapter 2, section 2.7	Human are reported to be the weakest link in information security. Therefore, end user roles and responsibilities help an organisation to manage data access and information assets and to properly control security risks.
4. To effectively respond to detected cybersecurity attacks	Chapter 4, section 4.2.5	Banking institutions should be able to respond accordingly to any cyber-attacks in order to minimise the damage.
5. To recover from cybersecurity attacks	Chapter 4, section 4.2.5	It is important for banking institutions to establish an effective remediation plan in order to recover from cybersecurity attacks.
6. To comply with organisational, national, industry and international guidelines, regulations and laws	Chapter 4, section 4.2.4	In the banking industry there are certain laws, regulations and compliance requirements in which the banking institutions are obliged to comply to in order to avoid legal penalties.

5.4 Design and Development

The researcher reviewed existing literature to obtain secondary data that provided the foundation for the proposed framework. In this regard, NIST cybersecurity framework, ISO/IEC27001: 2013 and the Framework for the Governance of Information Security in Banking System frameworks were used as guidelines. These three frameworks were selected based on

the needs and core security areas that are essential for the banking institutions. An analysis of the strength and weaknesses of these frameworks is given in section 2.7. Given the issues discovered from primary data in the context of the banking sector in Namibia, it became necessary to select three most appropriate frameworks and use them as the foundation of the proposed cybersecurity framework for the banking sector of Namibia.

Table 5.5 provides explanations why NIST cybersecurity framework, ISO/IEC27001 and the framework for the Governance of Information Security frameworks were selected as a basis/foundation of the NBCF.

Table 5.5 Summary of the three selected frameworks

Criteria	NIST (National Institute of Standards and Technology) cyber security framework	ISO/IEC27001	A Framework for the Governance of Information Security in Banking System
Relevance/Suitability to the banking sector	NIST helps organisations manage and reduce cybersecurity risk to critical infrastructure and industrial control systems which makes it more relevant to banking institutions. Furthermore, its risk-based iterative approach helps an organisation to manage security risks in real time.	ISO/IEC 27001 provides requirements for an ISMS. It allows any type of organisations to manage the security of assets such as financial data. With 14 domains and over 139 controls an specified in ISO/IEC27001: 2013 addresses comprehensively the needs of banking sector when it comes to information systems management.	Its general approach is information security governance program. Effective information security cannot be realised without governance. Information security governance comprises of the tools, personnel and business processes that ensure that security is implemented to meet an organisation's precise needs. This is particularly essential in the banking sector where governance helps to

			ensure that an organisation has the proper controls to mitigate security risk.
--	--	--	--

5.4.1 Components Identification

Numerous cybersecurity issues as illustrated by table 5.3 were identified from the literature review and data analysis. To solve these issues, a Namibia Banking Cybersecurity Framework which can serve as guidance to safeguard online transactions of financial data between banks and customers was developed. Thus table 5.6 explains how the framework components were identified from literature review and data analysis. The table summarises the components' function and relationships, importance and significance.

Table 5.6 Components relationship, importance, reference and significance

Component	Component function and relationship	Importance in Namibian Financial Banking Institutions	Reference to literature review and data analysis
Identification	<p>Identification of critical assets. <i>This is the first component and it relates to the classification, protection, detection, recovery and compliance components.</i></p> <p>Activities in this component include: Identifying assets e.g. data, users/people, networks, servers, etc.; asset inventory; identifying vulnerabilities; identifying threats; risk assessment; and identifying risk mitigation strategies which are aligned with the organisational strategic goals and objectives; cyber breach simulations.</p> <p>Asset identification is important for an organisation's capacity to quickly connect various sets of information about assets. The purpose of asset identification is to acquire all required information about an organisation's assets ahead of time so that it may be used to respond to a threat affecting that asset. Asset identification leads to classification of assets and subsequently to the deployment of required protection mechanisms.</p>	<ul style="list-style-type: none"> • Critical assets are assets that sustain the business e.g. data, users/people, networks, servers, etc., Knowledge of their existence helps to proactively gather all necessary information about the assets that can be useful in responding to a threat affecting that asset. It also helps in identifying risk mitigation strategies which are aligned with the organisational strategic goals and objectives. • All critical assets associated with information and information processing facilities should be identified and an inventory should be maintained. • Critical assets have a high risk of failure and major consequences such as reputation concerns, legal penalties and compliance issues. • Therefore, it is important for banking institutions to have an understanding of its critical assets. 	<p>According to Security Intelligence 2016, many banking organisations neither identify nor classify data based on sensitivity and criticality (refer to chapter 4, section 4.2.3). As a result, banking organisations lack an understanding of which information assets matter to them most so as to provide appropriate security. Therefore, the identification of critical assets becomes the first step towards data protection and privacy. In addition, this can serve the institution from legal penalties due to compliance to industry regulations and laws. Identification component is inspired and adopted from NIST framework and the Governance of Information Security in Banking System.</p>

		<ul style="list-style-type: none"> It is also important to perform vulnerability assessments in order to effectively identify risks and vulnerabilities in computer networks, systems, hardware, applications, and other parts of the businesses. 	
Classification	<p>Classification of critical assets. <i>This component relates to the identification, protection, detection and compliance components.</i></p> <p>Activities in this component include: Classifying assets; classifying risks; risk prioritization; defining data owners and data labelling.</p> <p><i>Asset classification</i> is used to identify the appropriate value and protection levels. Asset classification may be required by appropriate regulatory and industry-specific standards, which may require classification of different data attributes. For example, the Cloud Security Alliance (CSA) requires that data and data objects must comprise data type, jurisdiction of origin and residence, context, legal constraints, sensitivity, etc. Asset classification leads to assets protection and subsequently monitoring mechanisms.</p>	<ul style="list-style-type: none"> Classification of critical assets helps in understanding of which assets matter most to an organisation. Classification of critical assets that are key to the survival of the business. Classification of critical assets helps in applying appropriate levels of protection to information assets. 	<p>After identification of critical assets, they are classified. This component is adopted from ISO/IEC 27001: 2013 framework. According to this framework, Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. Furthermore, an appropriate set of procedures for information labelling should be designed and implemented in accordance with the organisation's information classification scheme.</p>

<p>Protection</p>	<p>Application of security controls to identified and classified critical assets.</p> <p><i>This component relates to identification, classification, detection and compliance components.</i></p> <p>Activities in this component include: access control; user awareness and training; training of cybersecurity experts (human factor - soft skills); data security; firewalls; IPS; antivirus; security policies; and system backups; role based access control (RBAC); public knowledge on information security practices etc.</p> <p>The quality of the overall protection of assets depend on the organisational environment, threats and vulnerabilities. Asset protection may comply with relevant regulatory and industry-specific mandates, which may require protection of different data sets.</p>	<ul style="list-style-type: none"> • Security controls and safeguards are applied in a systematic and consistent manner to critical assets based on the level of criticality of the asset to the organisation. This will enable the Namibian banking institutions to safeguard their assets in conjunction with the identified issue of data protection and privacy. 	<p>After classification, information assets are provided with appropriate level of protection. This component is adopted from NIST framework, ISO/IEC 27001:2013 and the framework for the Governance of Information Security in Banking System as described in chapter 2. According to NIST cybersecurity framework, organisations should develop and implement appropriate safeguards to ensure delivery of critical services. Examples of such safeguards include identity management and access control; awareness and training; training of cybersecurity experts; data security; information protection processes and procedures; maintenance; and protective technology. ISO/IEC 27001:2013 standard emphasizes on identifying organisational assets and defining appropriate protection responsibilities in an attempt of ensuring that information receives an appropriate level of protection in coordination with its criticality to the organisation. The Framework for the Governance of Information Security in Banking System advocates for increased third party security as such as cloud service providers since most banking institutions have the tendency of using technology services from which puts banking systems at risk.</p>
<p>Detection</p>	<p>Detection of the occurrence of a cybersecurity event/breaches.</p> <p><i>This component relates to identification, classification, protection and response components.</i></p> <p>Activities in this component include: vulnerability assessments anomalies</p>	<ul style="list-style-type: none"> • Security breaches should be detected in a timely fashion in order to reduce/stop the extent of the damage. 	<p>This component is adopted from NIST cybersecurity framework and the framework for the Governance of Information Security in Banking System as described in chapter 2. According to NIST cybersecurity framework, organisations should establish and implement relevant activities to detect the existence of a malicious cybersecurity event since this enables prompt mitigation/response to security threats, breaches and attacks. The framework for the Governance of Information Security in Banking</p>

	<p>and events logging and detection; IDS; security continuous monitoring; and detection processes.</p> <p>Detection is the practice of analysing the entirety of a security ecosystem in order to detect any malicious behaviour that could compromise the network or data confidentiality, integrity and availability. If a threat is detected, then response actions must be enacted to properly neutralise the attack/threat before it can pose damage to the asset/assets.</p>		<p>System emphasises on performing vulnerability assessments of network systems and applications periodically in order to detect security loopholes so as to act in a timely fashion.</p>
<p>Response</p>	<p>Responding to detected cybersecurity breaches as they occur. <i>This component relates to the detection and recovery component.</i></p> <p>Activities in this component include: response planning; communications channels; attack analysis; mitigation strategies; and improvements.</p> <p>Responding to security attack and threats is an important aspect of information security. The ability to recognise network intruders or other malicious adversaries in a timely fashion enables the organisation to effectively recover from security events and effectively mitigate damage.</p>	<ul style="list-style-type: none"> Containing the impact of a potential cybersecurity incident is essential to the survival of the business. Additionally, it helps in avoiding future incidents. 	<p>This component is adopted from NIST cybersecurity framework, ISO/IEC 27001:2013 and the framework for the Governance of Information Security in Banking System as described in chapter 2. NIST framework advocates on developing and implementing appropriate activities to take action regarding a detected cybersecurity incident. ISO/IEC 27001:2013 framework advocates that procedures should be designed to provide a timely, effective and orderly response to information security incidents. The framework for the Governance of Information Security in Banking System emphasises performing dynamic simulations to threats in order to assess incidence response readiness and effectiveness.</p>

<p>Recovery</p>	<p>Recovering from cyber-attack incidents. <i>This component relates to identification and response components.</i></p> <p>Activities in this component include: Executing Disaster Recovery Plan/Business Continuity Plan; disaster recovery documentation; Incidence response activities; forensic evidence gathering; restore plans; data isolation; and compliance issues etc.</p> <p>Recovery helps to create an effective system to manage business disruptions and to be able to contain the impact of a potential cybersecurity incident.</p>	<ul style="list-style-type: none"> Recovering from cyber-attack incidents helps the organisation to resume services after a disruption in order to reduce losses or avoid legal penalties. A recovery plan also helps the business in defining and meeting the defined Recovery Point Objective (RPO) and Recovery Time Objective (RTO). This helps the organisation to minimise data loss and service loss. 	<p>This component is adopted from NIST cybersecurity framework, ISO/IEC 27001:2013 and the framework for the Governance of Information Security in Banking System as described in chapter 2. NIST framework focuses on the development and implementation of appropriate activities to maintain plans for resilience and to restore any capabilities or services that was impaired due to a cybersecurity incident. ISO/IEC 27001:2013 standard emphasizes on establishing organisation's business continuity management systems. The framework for the Governance of Information Security in Banking System focuses on initiation of action plans and mobilisation of resources to remediate following a cyber-incident.</p>
<p>Compliance</p>	<p>Compliance to various industries, national and international laws and regulations. <i>This component relates to identification, classification and protection components.</i></p> <p>Activities in this component include: Compliance to applicable legislation intellectual property rights; compliance with security policies and standards and operation procedures; corporate governance; ethical conduct; trust and auditor security.</p>	<ul style="list-style-type: none"> Banking institutions are subjected to comply with a number of industry, national and international laws and regulations. Failure to adhere to some of these laws and regulations may result in serious negative consequences for the business operations. 	<p>This component is derived in reference to ISO/IEC 27001:2013 standard. According to this standard, an organisation should avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements through compliance. Some of the legislation, regulations and laws that the Namibian banks must comply to include BoN BID-30; PCI-DSS; Financial Intelligence Act (FIA); Know Your Client (KYC); Anti-Money Laundering (AML); Protection of Personal Information Act (POPI Act); and GDPR.</p>

	To ensure secure operations and the proper protection of sensitive data, financial institutions are normally expected to comply with local and international regulatory security compliance requirements.		
--	---	--	--

Table 5.7 provides a list of identified security issues through the literature review and interviews and an overview of how the proposed framework will address these issues.

Table 5.7 Identified cybersecurity issues

Identified Issues:	Solutions as addressed in the framework
Data protection and privacy	An organisation should comply with relevant laws and regulations regarding data protection and privacy by implementing appropriate security controls. This issue is catered by the proposed framework in the following components: compliance and protection.
Human factor - soft skills	Soft skills are an essential aspect of non-technical security controls which support technical security controls. This issue is catered for by the proposed framework in the following component: protection.
Principle of Least Privilege (POLP)	An organisation should implement appropriate access control mechanisms that address the issue of Principle of Least Privilege (POLP) such as role based access control (RBAC) in order to reduce the risk of data leaks. This issue is catered for by the proposed framework in the following component: protection.
Public knowledge on information security practices	An organisation should make sure that the public is aware of information security concerns and issues by providing education/instructional events. This issue is catered for by the proposed framework in the following component: protection.
Aspect of disaster recovery documentation	An organisation should create and document business continuity and/or disaster recovery plans to enable provision of services in case of any unforeseen circumstance. This issue is catered for by the proposed framework in the following components: response and recovery.
Cyber breach simulations	An organisation may conduct cyber breach simulations as way to identify system/network/process vulnerabilities in order to mitigate risks. This issues is catered for by the proposed framework in the following component: identification.
Corporate governance	Good corporate governance may lead to compliance with relevant laws and regulations to avoid legal penalties. This issue is catered for by the proposed framework in the following component: compliance.
Ethical conduct	An organisation may avoid legal penalties by conducting businesses activities ethically. This issue is catered for by the proposed framework in the following component: compliance.

Trust	An organisation should build trust with its stakeholders by complying to relevant laws and regulations. This issue is catered for by the proposed framework in the following component: compliance.
Auditor security	This is an aspect of effective information security. This issue is catered for by the proposed framework in the following components: protection and compliance.

Description of the proposed NBCF

The proposed framework comprises of seven components with corresponding subcomponents. The seven components are identification, protection, detection, response, recovery and compliance. The subcomponents are specific areas of security domains with corresponding security objectives which cover a wide variety of security elements and key areas. Lastly, activities are security tasks which can be implemented or carried out to achieve corresponding security objectives.

The proposed NBCF provides cybersecurity risk management strategies to both technical and managerial audiences. The proposed framework advocates for cyber resilience with the main focus on cybersecurity risk management. By implementing the framework, organisations may be able to build cyber resiliency, where systems and operations are designed to detect cyber threats, respond to and recover from cyber events in order to minimise business disruption and financial losses.

IDENTIFICATION

In this category, the business identifies its critical functions, information assets and corresponding risks which influence strategic goals and objectives of the organisation. Information assets are all data items which all organisations depend on to carry out their businesses. Common criteria include the asset’s monetary value, legal standing and importance to the organisation. This allows an organisation to concentrate and prioritise its activities in accordance with its risk management strategy and asset value and business requirements. A subcomponent to this component is asset management. Examples of security activities in this

component include: asset inventory and management; risk assessment and risk management strategies. After identifying assets, they should be classified before implementing appropriate levels of security controls.

CLASSIFICATION

The objective of information classification is to ensure that all information assets (whether in physical or digital form) have an appropriate information classification applied. Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. In addition to that, a suitable set of information labelling procedures should be designed and applied in accordance with the organisation's information classification scheme. Information assets are protected to guard against unintended disclosure, unauthorised modification, or destruction of an asset which might affect security. Classification extends across confidentiality, integrity and availability of assets. Each of these three principles is assessed to ensure that the classification of the assets is done in a way that is meaningful to the organisation. Business information, assets and data are classified according to the level of confidentiality, sensitivity, value and criticality. Information may be classified and labelled as highly restricted, confidential, internal use only, and public. After classification, assets are subjected to an appropriate level of protection and defence.

PROTECTION

When deciding on the suitable level of classification, it is crucial to balance between the protecting such information assets from potential harmful disclosure and disseminating it for effective use. Some information can be valuable, thus access to it should be controlled as such information assets are restricted and the information is subject to specific handling instructions. The higher the classification, the more stringently access is controlled and limited. Appropriate security measures and controls are developed and implemented to safeguards information assets. Both logical and physical security measures can be applied. These includes: access control and identity management, user awareness and training, training of cybersecurity experts, network security, data Security; Information handling procedures and use of security

technologies. After implementing appropriate levels of protection and defence to assets, the next aspect is to detect malicious activities/attacks in a timely fashion.

DETECTION

In this category, appropriate procedures and technologies implemented are used to identify the incidents and potential occurrences of cybersecurity events. This enables timely discovery of cyber security events and potential attacks. Activities within this category include: implementing detection systems, monitoring (users, networks, and security controls) and detection processes. After detecting malicious activities/attacks, an organisation should be able to respond to the detected malicious activities in order to minimise damage or business disruptions. This includes identifying malware activity characteristics by inspecting detection sources such as intrusion prevention systems, antivirus software and Security Information and Event Management (SIEM) technologies.

RESPONSE

An incident response plan should be implemented to address suspected data breaches. An incident response plan guides how an organisation will react in the event of a security breach. The aim is to minimise damage, mitigate breach-related costs and reduce disaster recovery time. An organisation should be able to contain the impact of a potential cybersecurity breach. Examples include creating an incident response plan, incident recovery team, determine the critical components, communications plan and mitigation strategies. After responding to malicious activities/attacks, an organisation should be able to recover by resuming business activities that were disrupted.

RECOVERY

This involves adopting processes or a set of procedures and appropriate activities to restore any services disrupted by a cybersecurity incident. An organisation should be able to mitigate an attack with a meaningful and practiced incident response plan. This also involves executing the

organisation disaster recovery plan to resume business activities while restoring the normal processes.

COMPLIANCE

Compliance means ensuring, complying or adhering to the minimum of the security-related requirements. An organisation may be required to comply with legal requirements or with security policies and standards and technical compliance. In the financial sector, there are certain national regulations or several international compliance requirements in which organisations are obliged to comply to. In this framework, compliance is implemented in three of the categories as there can be certain legal or industry regulations that should be adhered to.

5.4.2 Components Relationships

This section confers the relationships between the framework components. It explains in detail the relationships and interconnectedness of the components. R - represents a relationship.

The framework components are abbreviated as follows:

- ❖ Identification (I)
- ❖ Classification (CL)
- ❖ Protection (P)
- ❖ Detection (D)
- ❖ Response (RES)
- ❖ Recovery (REC)
- ❖ Compliance (COM)

Component 1: Identification

Relationship 1 (R1): Identification of critical assets is the first step in this framework. This step provides guidance of classification of assets and identifying risk mitigation strategies which are aligned with the organisational strategic goals and objectives. Assets are classified according to

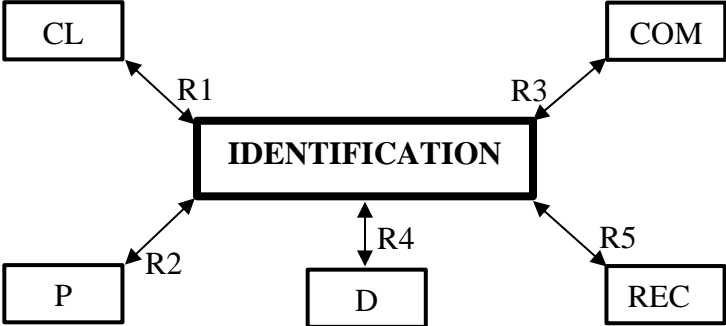
the level of confidentiality, sensitivity, value and criticality. Asset identification leads to the classification of assets and subsequently to the deployment of required protection mechanisms. The objective of data classification is to ensure that all identifiable information assets which belong to the organisation, whether in a digital or physical form, have an appropriate level of information classification applied to them. Every organisation must be aware of the value of the information contained in the information assets it possesses and should implement appropriate controls to ensure that protection is given to information assets corresponding to the classification.

Relationship 2 (R2): The goal of asset identification is to proactively gather all the necessary information about an organisation's assets that can be useful in protecting assets against threats affecting them. Every time identified critical assets are generated, deliberation should be made as to whether they require additional protection.

Relationship 3 (R3): In addition to regulatory requirements such as on data protection, organisations need to implement and maintain strong standards for the protection of the identified assets and also comply to certain legal or industry regulations as applicable/necessary.

Relationship 4 (R4): Detection is the practice of analysing the entirety of a security ecosystem to identify any malicious activity that could compromise the network or data integrity. Hackers and insiders always find ways of exploiting various critical assets inside organisations. Organisations therefore need to develop schemes of identifying and tracking critical information assets. The organisations should ensure that it has a reliable and timely identification and tracking system of its critical assets. Once you know where your critical assets reside, you will be able to detect any malicious activities and take appropriate protective measures and react precisely to threats. Detection approaches include but are not limited to identifying malware activity characteristics by inspecting detection sources, such as IPS, antivirus software and SIEM technologies.

Relationship 5 (R5): Once critical assets such as data, users/people, networks, and servers are identified, it is also vital to identify vulnerabilities and threats to these assets and the recovery strategies from these threats. It is important to understand the business and the resources that support critical functions, as well as the associated cybersecurity risks since this enables the organisation to focus and prioritise its activities, consistent with its recovery strategies and business requirements.



Component 2: Classification

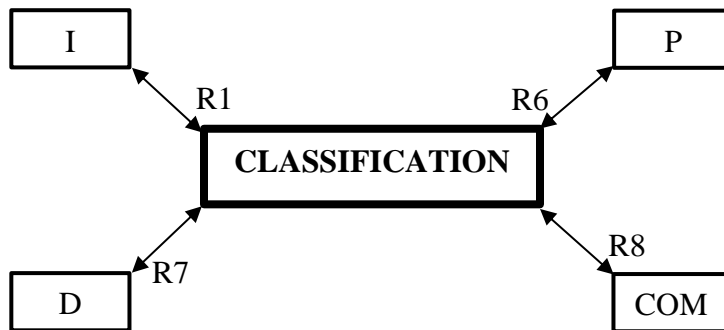
Relationship 1 (R1): As defined under component 1.

Relationship 6 (R6): This classification will be used to guide the implementation of suitable security controls and other mechanisms to protect the classified information from being manipulated, leaked or from becoming unavailable. Throughout the process of determining the appropriate level of classification, controls should be implemented to protect these assets from harmful disclosure and possible misuse and unauthorised dissemination. Security controls and safeguards are applied in a systematic and consistent manner to critical assets based on the level of criticality of the asset to the organisation.

Relationship 7 (R7): In determining the appropriate level of classification, there is a requirement to be able to detect potential threats and vulnerabilities to the assets as the assets require substantial degree of protection. If a threat to the identified and classified critical assets is

detected, then response actions must be enacted to properly neutralise the attack/threat before it can pose damage to the assets.

Relationship 8 (R8): Lastly, at this point, regulatory or legislative issues may also impact the security classification of the information and this needs to be considered.



Component 3: Protection

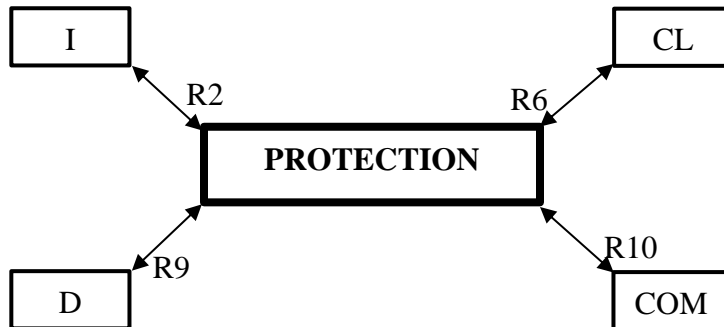
Relationship 2 (R2): As defined under component 1.

Relationship 6 (R6): As defined under component 2.

Relationship 9 (R9): It is vital to implement suitable protections to assure the delivery of critical infrastructure services that will aid in detecting and containing the impact of a potential cybersecurity event. Detection entails implementing appropriate activities to timely identify and discover security breaches in order to reduce and stop the extent of the damage, and by doing so critical assets will be protected.

Relationship 10 (R10): While critical data is being protected, compliance with security policies and standards and operation procedures remain priority as well. Thus, asset protection may be

in compliance with relevant regulatory and industry-specific mandates which may require the protection of different data sets.



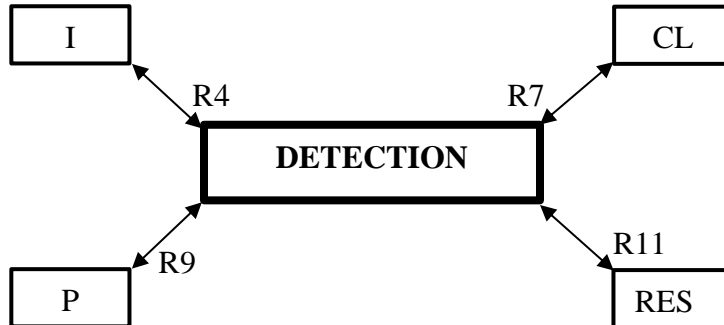
Component 4: Detection

Relationship 4 (R4): As defined under component 1.

Relationship 7 (R7): As defined under component 2.

Relationship 9 (R9): As defined under component 3.

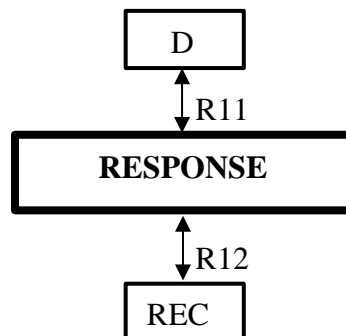
Relationship 11 (R11): Detection of cybersecurity incidents is key to the protection of organisational critical assets. Every organisation must implement cybersecurity strategies and develop an incident response plan in order to monitor the network and detect those cyber-attack attempts as early as possible. This will result in navigating those attacks safely and successfully. Responding to cybersecurity events enables the recovery of systems. This involves adopting processes or a set of procedures and appropriate activities to restore any services disrupted by a cybersecurity incident. The ability to detect network intruders or other malicious adversaries in a timely fashion enables the organisation to effectively recover from security events and effectively mitigate damage.



Component 5: Response

Relationship 11 (R11): As defined under component 4.

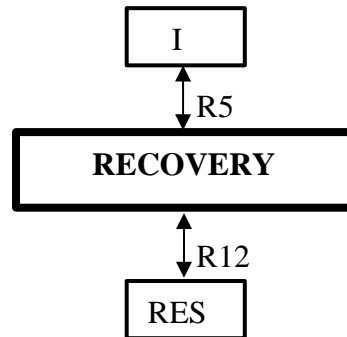
Relationship 12 (R12): An organisation needs to implement appropriate controls to take action towards a detected cybersecurity incident which should support the ability to contain the impact of the detected cybersecurity event. Recovery entails implementing appropriate activities to maintain plans for resilience and to restore business operations and services that were compromised due to the cybersecurity event. Every organisation needs to build cyber resiliency, where business operations and systems are designed to detect cyber threats and respond to and recover from cyber events to minimise business disruptions and financial losses and to withstand negative impacts. Recovering from a cyber-attack incident helps the organisation to resume services after a disruption in order to reduce losses or avoid legal penalties.



Component 6: Recovery

Relationship 5 (R5): As defined under component 1.

Relationship 12 (R12): As defined under component 5.



Component 7: Compliance

Relationship (R3), (R10) and (R8): As defined under component 1, 3 and 2. To ensure secure operations and the proper protection of sensitive data, financial institutions are normally expected to comply with local and international regulatory security compliance requirements. Asset identification, classification and protection efforts therefore need to be based on the known industrial and international laws and regulations.

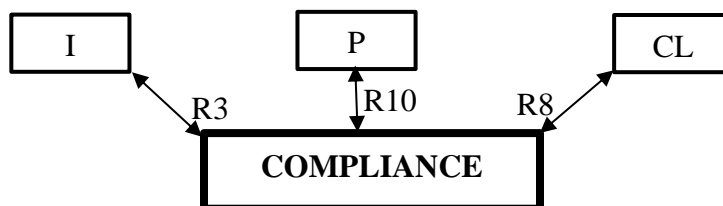


Figure 5.2 represents the proposed Namibia Banking Cybersecurity Framework (NBCF) with all the 7 components and security activities.

The proposed Namibia Banking Cybersecurity Framework (NBCF)

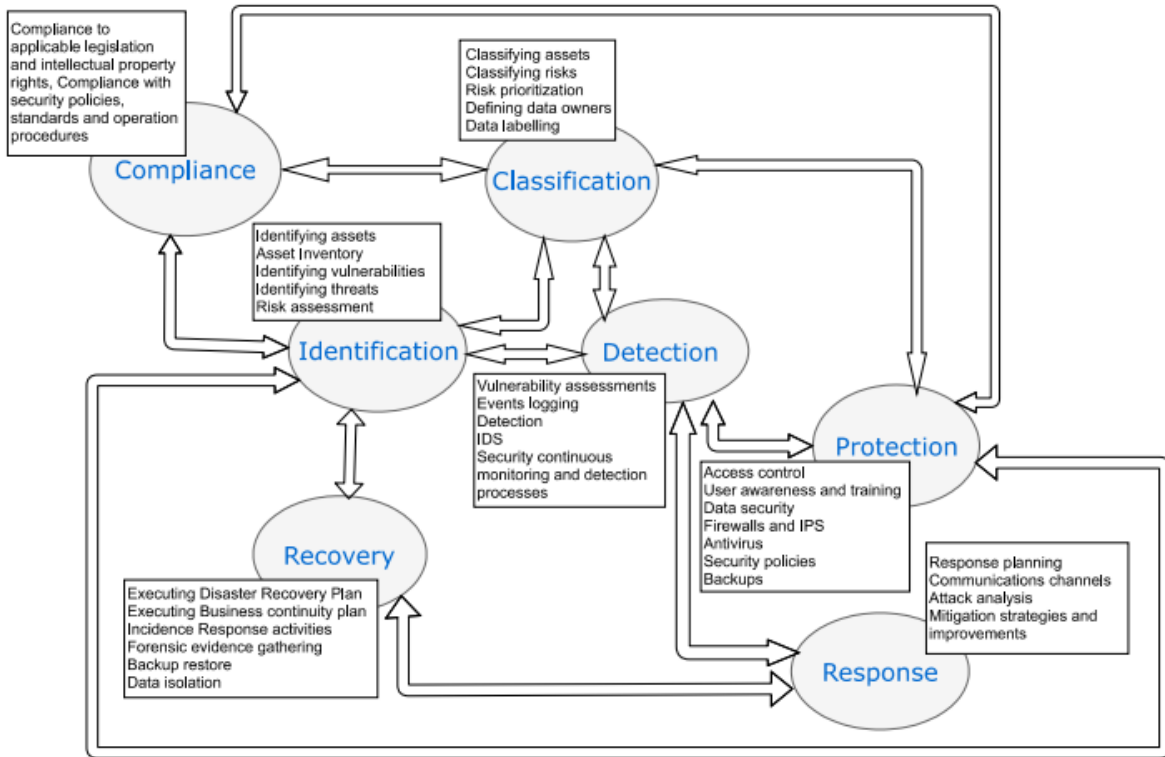


Figure 5.2 Proposed Namibia Banking Cybersecurity Framework (NBCF)

5.5 Demonstration

This section provides a demonstration of the capability of the proposed NBCF which was developed for Namibian Banking institutions. It comprises of seven components, i.e. identification, classification, protection, detection, response, recovery and compliance to cyber threats and vulnerabilities as presented in figure 5.2. Altogether, these framework components provide a high-level, strategic view of an organisation's cybersecurity risk management. To demonstrate the capability of the framework the following scenario is given.

Scenario:

With more than 20 years in existence, AG bank has more than 300 employees across its branches in Namibia. Over the years, AG bank has been implementing IT solutions that improve both the bank's efficiency such as Customer Relationship Management (CRM) and collaboration systems and client service (e.g. payment card processing, loyalty management systems, web and mobile banking apps for payment and access to bank accounts). However, AG bank's main challenge is the security of data, systems and services that are accessed by all bank employees in their needs or daily tasks, and end-customer access. In addition, AG bank is obligated to comply with organisational, national and international laws and regulations with regards to data security. Thus, AG bank needs guidance in applying a suitable cybersecurity framework in order to protect its customers' data and systems.

The purpose of this demonstration is to show how the banking institutions can apply the NBCF to their facilities. The goal of this scenario is to demonstrate the capabilities and adoptability of this framework through an illustrative based scenario on a real-world situation as given in section 5.5. The NBCF provides actionable activities that can be easily applied by any banking institution to enhance their cybersecurity. The steps that AG bank needs to follow in applying the proposed NBCF to their environment in order to secure its banking systems are explained in the following section.

Identifying all critical assets and functions of the banking institution

The first step is to identify information assets and risk mitigation strategies which are aligned with the organisational strategic goals and objectives. In this case, only few critical assets are considered for demonstration purposes as given below:

- Corporate data
- Customers data
- Websites
- Servers
- Software
- Network equipment
- Mobile Apps
- End user devices/ terminals

The outcome of this is an asset inventory list. Once this is in place, then a risk assessment has to be performed.

Risk assessment

The goal of risk assessment is to identify and describe the risk(s) associated with each asset and to analyse the potential impact of the risk to AG bank's strategic goals and objectives. For each asset, threats and vulnerabilities are identified, and these will be used to enumerate the risks posed to the asset. The probability and consequences of the risk is evaluated and categorised such as high, moderate, and low.

Table 5.8 shows the different risk assessment criteria.

Table 5.8 Risk assessment criteria

Criteria	Description
High risk	A condition that may cause frequent damages which may result in catastrophic data and equipment losses
Moderate risk	A condition that may cause damages which may result in mild catastrophic data and equipment losses
Low risk	A condition that is unlikely to cause damages, and even if it does, it results in only negligible damage

“Risk is the combination of the probability of an event and its consequence” (International Organization for Standardization [ISO] 31000:2009: Risk management). Following the identification of essential information assets, a risk assessment is carried out to identify vulnerabilities and threats, and define the likelihood of occurrence and the resulting impact. One can calculate the risk by evaluating the probable frequency of a particular event (likelihood of occurrence), as well as the probable impact of that event (ISO/IEC Guide 73:2009). The outcome of the risk assessment results can be used by business to provide control improvement and/or implementation guidance. For a risk assessment result where a key control does not exist, or it is poorly designed and/or not operating as intended, an adequate compensating control should be identified and should operate as intended.

Table 5.9 demonstrates a risk assessment process.

To calculate risk, the following formulae as explained above is used:

- Risk= **Likelihood of occurrence * impact**

Table 5.9 Risk assessment process

Information assets	Threats	Vulnerabilities	Impact	Likelihood of occurrence	Risk	Recommendation Control
Corporate and customers data, financial and economic information	Data theft, data deletion, data corruption	Weak passwords, Password sharing	High impact Trust and reputational loss	High	High risk Potential loss of customer data	Implement access control, Implement security policy
Servers	System failure	No backup servers	High impact All email, website servers will be unavailable	High	High risk Potential financial loss	Purchase backup servers, implement raid systems
Websites	DoDs attack, hackers	No pen - testing performed against the website for the past ten years	High impact Loss of customer trust	Moderate	High risk Loss of internet banking services	Configure firewalls, Intrusion Detection System (IDS), Demilitarized Zone (DMZ), IPS
Software	Virus	Patches not installed, expired antivirus	High impact Data availability	High	High risk Corrupt customer data	Patches must be installed and antivirus updated

Classifying Assets

Information assets are valuable resources to the organisation and they must be handled with care according to authorised handling procedures. According to ISO 27001, Information asset classification extends across confidentiality, integrity and availability of assets for any organisation. Information assets are classified based on their sensitivity levels and the impact to the organisation should that information be disclosed, altered, or destroyed without authorisation. Information classification aids in determining appropriate baseline of security

controls for safeguarding that Information asset. All organisational information assets should be classified into one of three classification tiers.

- Tier 1: **Public** – This type of information is intended for public consumption and disclosure and it is freely accessible to the public.
- Tier 2: **Confidential** – This type of information is not considered to be secret and it is generally not available to the public.
- Tier 3: **Restricted/Secret** – This type of information is required by law and/or regulation and the loss of confidentiality, integrity and availability of this information will have an adverse impact on the organisation’s mission, reputation, financial losses, safety or damage to employees and customers. Examples of restricted data might include Personally Identifiable Information (PII), proprietary information, and cardholder data (credit cards).

The financial sector has specific requirements that encourage organisations to classify information assets or data. Therefore, financial institutions are expected to comply with information privacy principles, policies regulations or legislation. Table 5.10 demonstrates the assets classification criteria inspired by NIST.

Table 5.10 Assets classification criteria

Classification Labels	Type of Information
Public	Websites
Confidential	Corporate and customers data, servers and software
Restricted/Secret	financial and economic information

Profiles are then created for each asset of the AG bank to determine the security precautions to be taken in order to protect them using the criteria described in table 5.11.

Table 5.11 Assets risk analysis

Low Risk	Moderate Risk	High Risk
<p>Data and systems are classified as low risk if they are not considered to be moderate or high risk, and:</p> <ol style="list-style-type: none"> 1. The data is intended for public disclosure, or 2. The loss of confidentiality, integrity, or availability of the data or system would have no adverse impact on the organisation’s mission, safety, finances, or reputation. 	<p>Data and systems are classified as moderate risk if they are not considered to be high risk, and:</p> <ol style="list-style-type: none"> 1. The data is not generally available to the public, or 2. The loss of confidentiality, integrity, or availability of the data or system could have a mildly adverse impact on the organisation’s mission, safety, finances, or reputation. 	<p>Data and systems are classified as high risk if:</p> <ol style="list-style-type: none"> 1. Protection of the data is required in compliance to law/regulation, or 2. The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on organisation’s mission, finances, or reputation.

Data and systems risk labelling

The identified critical assets are assessed for risk and the risk levels are determined as illustrated in table 5.12.

Table 5.12 Assets risk labelling

Asset	Risk Labelling
Corporate and Customers’ Data, Servers, Software, Mobile Apps	High
Website, Network equipment	Moderate
End user devices/terminals	Low

Prioritising assets and applying appropriate levels of protection

AG bank should prioritise and protect assets with high risk as presented in table 5.11 and 5.12. This requires the organisation to apply a level of security that is appropriate to the risks as presented in table 5.11. Table 5.13 shows the risk level labelled to the assets using priority levels.

Priority levels defined are:

- ❖ High risk – priority 1
- ❖ Moderate risk – priority 2
- ❖ Low risk – priority 3

Table 5.13 Assets risk levels

Asset	Risk level	Label
Corporate and Customers Data	1	High
Website	2	Moderate
Servers	1	High
Software	1	High
Website, Network equipment	2	Moderate
End user devices/ terminals	3	Low

Application of the appropriate level of protection

The appropriate level of protection is applied to assets in line with the recommendations specified in the risk assessment step one as shown in table 5.8. Controls for minimising the identified risks are identified during the risk mitigation phase. The controls are risk mitigation mechanisms that should decrease and/or avoid the occurrence of a risk event, detect risk event occurrence and reduce risk impact.

Table 5.14 Assets protection levels

Asset	Recommendation
Corporate & Customers Data	Implement access control, encryption, strong passwords, secure network, physical security, user awareness training and training of cybersecurity experts
Website, Network equipment	Configure firewalls, IDS, DMZ, IPS, secure network
Servers	Implement backup servers, implement raid systems, secure network, host based firewalls, IPS, physical security, strong passwords, encryption
Software	Install antivirus, configure firewalls, software updates
End user devices/ terminals	Implement access control and multi-factor authentication, strong passwords

Detection of security threats

Detection is the practice of analysing the entirety of a security ecosystem to identify any malicious activity that could compromise the network or data confidentiality, integrity and availability. If a threat is detected, then response actions must be endorsed to appropriately neutralise the attack before it can pose damage to the asset/assets. Methods that can be used by AG bank to detect threats are vulnerability assessments and events logging and detection, IDS, and security continuous monitoring as shown in table 5.15.

Table 5.15 Threats detection methods

Asset	Threat Detection
Corporate and Customers' Data	Events logging, IDS
Website, Network equipment	Web Vulnerability Scanning tools, vulnerability assessments, anomalies
Servers	Events logging
Software	Antivirus
End user devices/ terminals	Events logging

Once anomalies are detected then responses need to be invoked as presented in the next section.

Response to detected security threats and attacks

Responding to security attacks and threats is an essential aspect of information security. The ability of AG bank to recognise network intruders or other malicious adversaries in a timely fashion enables the organisation to effectively recover from security events and effectively mitigate damage. Table 5.16 shows activities that can be executed in response to detected security threats and attacks.

Table 5.16 Response activities to detected security threats and attacks

Detected Threats	Strategy	Activities
Data theft, data deletion, data corruption	Response planning	Develop the following: disaster recovery plan, disaster recovery team, recovery time objective and recovery point objective, incident response plan, incident response team
System failure	Communications channels	Define line of communication in response to threats and attacks
DoDs attack, hackers	Attack analysis	Attack analysis team and tools
Virus	Mitigation strategies	Document mitigation strategies

Recover compromised data and systems

Recovery helps to build an effective system to manage business disruptions and to be able to contain the impact of potential cybersecurity incidents. The following are strategies that AG bank can implement to recover compromised data and systems:

- Execute disaster recovery plan,
- Restore data back,
- Comply with relevant laws and regulations,
- Meet the recovery time objective and recovery point objective, and
- Document recovery procedure for future use.

Compliance to laws and regulations

AG bank is obliged to comply with applicable legislations and laws with regards to corporate and customer data security. For example, AG bank needs to comply to General Data Protection Regulation, PCI-DSS, and BoN BID-30 regulations. Compliance to such legislation and laws should be measured and maintained, and continually updated from changes at all levels. In addition, AG bank should comply with security policies and standards and operation procedures. To ensure secure operations and the proper protection of sensitive data, AG bank is required normally to comply with local and international regulatory security requirements.

5.6 Evaluation

The usability, adaptability and relevance of the proposed Namibia Banking Cybersecurity Framework are evaluated in this section. According to Hevner, March, Park, and Ram 2004), these phases allow for the demonstration of the artefact performance against the set matrices.

5.6.1 Objectives of the Evaluation

The objectives of the Namibia Banking Cybersecurity Framework evaluation are as follows:

- To determine the significance of the proposed framework in the Namibian context,
- To determine the relevance of the framework in the Namibia Banking Institutions, and
- To determine the applicability of the framework in the Namibia Banking Institutions.

A number of research studies have comprehensively used various evaluation techniques such as case studies, field experiments, and expert reviews. This study adopted the expert review technique in order to evaluate the usability and adaptability of the framework.

The primary purpose of the evaluation, in addition to gaining insights into the significance of the framework is to enable the determination of its merit, worth and relevance using a set of metrics. The evaluation tool was designed with reference from literature and a pilot study was conducted. Qualitative data analysis methods were used to analyse the data gathered.

5.6.2 Expert Review

An expert review is a type of inspection that is designed to determine the usability or the flaws of the framework. The review was carried out by a small group of field experts who analysed the framework or service to identify any potential usability issues. According to Ling and Salvendy (2005) and Nielsen and Molich (2009), expert reviews provide the following advantages:

- They provide the chance to make changes in the early stages of the process;
- Experts can identify a variety of issues in many aspects of a product. They assess the product as a whole, rather than focusing on only one or a few scenarios. They take a broader view and uncover issues that the researcher may have missed;
- Expert reviews provide a complete picture of the product. This is far more beneficial than getting feedback on a single scenario;
- Expert reviews are a more efficient way to evaluate a product, system or service; and
- Expert reviews are far more cost effective compared to field experiments. Reviews can be carried out multiple times during a project giving the advantage of expert knowledge and expertise to identify flaws and provide recommendations for improvement to a product, system or service.

About Experts

The criteria for the selection of expert reviewers was based on the following:

- Academic qualification: Experts were expected to have a degree related to Computing or IT, Cybersecurity, Risk Analysis and Information Systems.
- Industrial certification: Experts were expected to have an industrial certification related to Computing or IT, Cybersecurity, Risk Analysis and Information Systems, preferably Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), Project Management Professional (PMP), Certified in the Governance of Enterprise IT (CGEIT), CompTIA Security+.

- Industrial experience: Experts were expected to possess industrial experience in Computing or IT, Cybersecurity, Risk Analysis and Information Systems preferably within the banking sector.
- Job Position: Experts were expected to hold a position related to Cybersecurity, Information Security, Network Security, IT Risk or any IT related position preferably within the banking sector.

5.6.3 Framework Evaluation Tool

An online google form evaluation questionnaire was developed. The questionnaire was reviewed by the supervisors and pilot tested by three experts to validate the construction and understanding of the questions before they were deployed to a wider group of reviewers. A convergence test was done to ensure that it achieved the research objective of developing a cybersecurity framework to guide financial institutions in safeguarding online transactions of financial data between banks and customers as well as to ensure it validated the framework objectives as set in section 5.3.

The tool consisted of four sections where the first section introduced the purpose of the evaluation and presented the ethical considerations of the tool. The second section focused on the demographic information of experts; it evaluated the work experience of the reviewers. The third section of the evaluation focused on understanding the suitability of the NBCF framework in the Namibian banking institutions and appropriateness, applicability and relevance of the component constructs and framework. It also focused on understanding the importance of the components in providing cyber resilience in banking institutions. Lastly, the fourth section evaluated the whole structure of the framework. It focused on the framework relationships, clarity, and the completeness of the framework. The outcomes are presented in section 5.6.4.

5.6.4 Findings of the Evaluation

I. Demographic information of the reviewers

The reviewers demonstrated quite a high level of educational qualifications as 50% of the reviewers have at least a Master’s degree, 10% have a PhD, 20% have an Honours degree and the other 20% at least holds a first degree. All the reviewers except one indicated that they hold relevant professional certifications ranging from CISM, CompTIA Security+, CISA, Certified Ethical Hacker (CEH) pending, CISSP, and CRISC. The participants hold different roles in their organisations with 30% working as Information security managers/specialists, 20% are IT Risk Specialists/Analysts, 20% are Network Security Specialists, 10% are Chief Information Security Officers (CISO), 10% are heads of information security and lastly the other 10% work as lecturers. Lastly, the reviewers demonstrated a very advanced information security and cybersecurity knowledge level and experience as 60% have up to 5 years of experience in the profession while the other 20% have 6-10 years of experience and the remaining 20% has more than 20 years of experience in the profession. Table 5.17 summarises the reviewers’ demographic information.

Table 5.17 Expert Reviewers’ Profiles

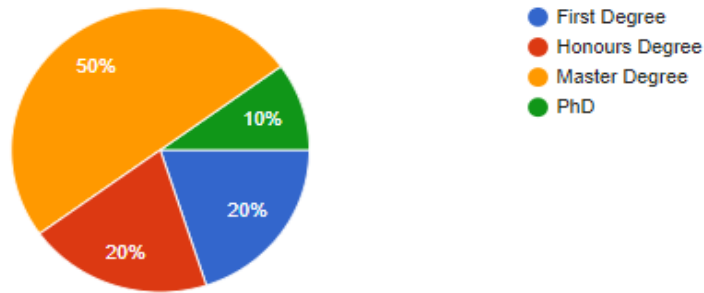
Respondents	Educational Qualification	Professional Certifications	Role	Years of Experience
Reviewer 1	PhD	CISM	Lecturer	6-10 years
Reviewer 2	First Degree	CompTIA Security+	SOC Analyst	0-5 years
Reviewer 3	Master’s Degree	CISA	IT Risk Specialist/Analyst	6-10 years
Reviewer 4	Honours Degree	CISA	Information Security Manager/Specialist	0-5 years
Reviewer 5	Master’s Degree	None	Academic	0-5 years
Reviewer 6	First Degree	CISA	Information Security Manager/Specialist	0-5 years
Reviewer 7	Honours Degree	CISA	IT Risk Specialist/Analyst	0-5 years
Reviewer 8	Master’s Degree	CEH pending	Information Security Manager/Specialist	0-5 years
Reviewer 9	Master’s Degree	CISSP, CISM, CISA, CRISC	Chief Information Security Officer	More than 20 years

Reviewer 10	Master's Degree	CISM, CISA, CRISC	Chief Information Security Officer	More than 20 years
-------------	-----------------	-------------------	------------------------------------	--------------------

Figure 5.3 represents the reviewers' demographic details in terms of education and professional certifications.

1. Educational qualification

10 responses



2. Relevant Professional Certifications (Choose all applicable)

10 responses

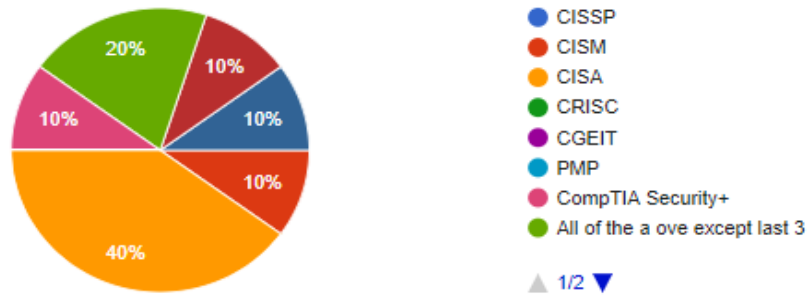
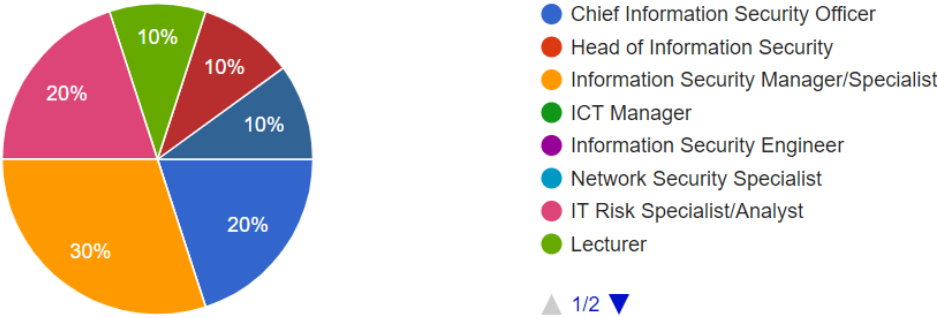


Figure 5.3 Reviewers' Demographic details: Education and Professional Certifications

Figure 5.4 represents the reviewers' demographic details with regards to role and experience

3. Please indicate your role in your organisation (choose one)

10 responses



4. Please specify your IT Risk or Information Security years of experience

10 responses

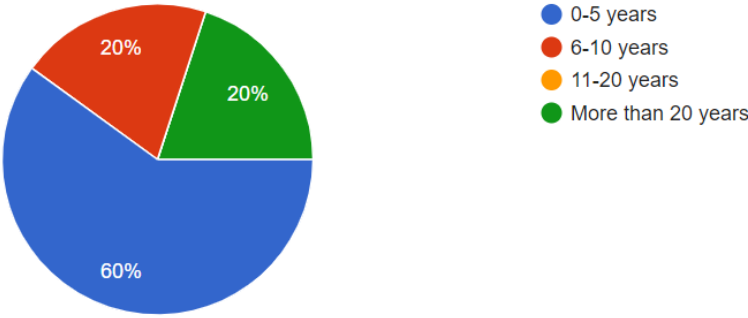


Figure 5.4 Reviewer's Demographic details: role and experience

II. Evaluation of the NBCF Framework

The NBCF evaluation focused on evaluating the relevancy and usability of the framework and how the banking institutions could adopt the framework to their facilities in order to enhance their cybersecurity posture. Table 5.18 presents the reviewers' responses on the framework appropriateness and relevance.

Table 5.18 Reviewers’ responses on framework appropriateness and relevance

Respondents	To what extent do you agree that the framework will support identification of critical information assets inventory and business functions?	To what extent do you agree that the framework will help in detecting cybersecurity attacks in the banking sector in a timely manner?	To what extent do you agree that the framework will support in protecting human resources of the banking sector?	To what extent do you agree that the framework will support in protecting information system assets of the banking sector?	To what extent do you agree that the framework will help banking institutions in effectively responding to detected cybersecurity attacks?	To what extent do you agree that the framework will help banking institutions in recovering from cybersecurity attacks?
Reviewer 1	Agree	Agree	Agree	Agree	Agree	Strongly Agree
Reviewer 2	Agree	Strongly Agree	Strongly Agree	Agree	Strongly Agree	Strongly Agree
Reviewer 3	Strongly Disagree	Strongly Disagree	Strongly Disagree	Strongly Disagree	Strongly Disagree	Strongly Disagree
Reviewer 4	Strongly Agree	Neutral	Neutral	Agree	Agree	Agree
Reviewer 5	Agree	Neutral	Strongly Agree	Strongly Agree	Agree	Agree
Reviewer 6	Neutral	Agree	Disagree	Agree	Neutral	Agree
Reviewer 7	Disagree	Disagree	Agree	Neutral	Neutral	Neutral
Reviewer 8	Neutral	Agree	Agree	Agree	Neutral	Agree
Reviewer 9	Neutral	Agree	Neutral	Agree	Agree	Neutral
Reviewer 10	Neutral	Agree	Neutral	Agree	Agree	Neutral

Firstly, 60% of the reviewers indicated that the framework will support the identification of critical information assets inventory and business functions, while 40% remained neutral. With regards to detecting cybersecurity attacks in the banking sector in a timely manner, 77% of the reviewers showed that the framework will be effective while 23% chose to remain neutral. To add to that, 67% of reviewers indicated that the framework will support in protecting human resources and information system assets of the banking sector while 33% pose a neutral view. As clearly revealed in the literature review (section 2.8), that the focus of the majority of the framework studies contain only few cybersecurity features and no attention was given to the other essential features such as human factors. Additionally, 77% of the reviewers also indicated that the framework will help banking institutions in effectively responding to detected cybersecurity attacks. Lastly, 77% of reviewers also indicated that the framework will help banking institutions in recovering from cybersecurity attacks. With reference to literature review (section 2.8), it is documented that it is worthwhile to bring together these stakeholders in the banking industry particularly in Namibia to tackle these cyber risks and build a theoretical standpoint for cyber security, consider implementation feasibilities in the banking sector as well as ways to evaluate cyber threats and make it sustainable.

Comments

Question: If you have any comments for question 5, please elaborate.

Table 5.19 further presents the reviewers' responses on the framework appropriateness and relevance.

Table 5.19 Reviewers' comments on the appropriateness and relevance of the framework

Reviewer	Comments
Reviewer 2	I do agree that the framework covers all areas that is required for a secure banking system and its infrastructure, but how effectively these many factors are implemented will determine how good this is as a framework. The controls that's put in place will determine if it's a good framework instead being a cybersecurity guide.
Reviewer 4	The framework will greatly assist with the identification of assets as well as the response and recovery of attacks. However, the timely response and protection of human resource can highly be influenced by behaviour and circumstances, constant awareness and testing will be of great influence.
Reviewer 5	Detection of cybersecurity attacks as presented in the framework is more technical and excludes trained experts. Not all attacks can be detected by technological solutions. There also needs to be a component on Security Expert training, this can be done addition another component or integrated into the existing components, especially under Protection, and Response.
Reviewer 7	1. The framework fails to reference core regulations within the Namibian banking industry. 2. The influence of strategic goals and objectives of an organization are not taken into consideration with identifying critical assets. 3. Like NIST and ISO, MITRE ATTACK framework is well established knowledge base that would contribute greatly to the detection and response sections of the NBCF.
Reviewer 9	More information is needed on the seven areas as it depends on what the framework proposes should be done. What is new from this framework to other like NIST CSF?

The reviewers' comments were analysed by the researcher as presented:

Reviewer 2 comment: I agree with the comment that the controls that are put in place will determine if it's a good framework instead of being a cybersecurity guide. However, table 5.24 which is the overview of the Namibia Banking Cybersecurity Framework stipulates the activities which are controls to be implemented for every framework component.

Reviewer 4 comment: I agree with the comment that the framework will greatly assist with the identification of assets as well as the response and recovery of attacks. The

reviewer also indicated that the timely response and protection of human resources can be highly influenced by behaviour and circumstances, constant awareness and testing will be of great influence. It is therefore important to note that the protection component had already included user awareness and training as one of the controls to be implemented within the protection component. Refer to Figure 5.2 - Proposed Namibia Banking Cybersecurity Framework (NBCF).

Reviewer 5 comment: I agree with the comment that the detection of cybersecurity attacks as presented in the framework is more technical and excludes trained experts. Not all attacks can be detected by technological solutions. There also needs to be a component on Security Expert training, and this can be done in addition to another component or integrated into the existing components, especially under protection, and response. I will therefore refine the framework by adding “training of cybersecurity experts” to the protection component. It is worth noting that although the protection component had already included user awareness training, this was just general cybersecurity training for all staff and not necessarily targeted “cybersecurity expert training”.

Reviewer 7 comment: The reviewer highlighted that the framework fails to reference core regulations within the Namibian banking industry, like NIST and ISO. MITRE ATTACK framework is a well-established knowledge base that would contribute greatly to the detection and response sections of the NBCF. I however, disagree with the first comment as the literature review, section 2.7, has evaluated the existing cybersecurity frameworks which included BoN BID-30, NIST and ISO/IEC 27001:2013. With regards to the second comment which is the influence of strategic goals and objectives of an organisation which are not taken into consideration with identifying critical assets, I agree that I have underlooked that aspect to some extent and it will partially be incorporated in the framework refinement and it will be added under the identification. Under the identification component, one of the control is identifying risk mitigation strategies. It will therefore be

refined by saying, “identifying risk mitigation strategies which are aligned with the organisational strategic goals and objectives”.

It is therefore worth noting that the influence of strategic goals and objectives of an organisation should be taken into consideration in the adoption and implementation of the framework as a whole. Organisational strategies can take many forms and they can go into varying levels of detail, depending on the particular organisation’s objectives and the level of their cybersecurity appetite. Thus, there are various agreed definitions of what constitutes an organisational cybersecurity strategy and this framework provides a foundation of the steps, programmes and initiatives that an institution will undertake to protect its information assets and, in the process, increase its cybersecurity resilience.

Reviewer 9 comment: The reviewer indicated that more information is needed on the seven areas as it depends on what the framework proposes should be done. The reviewer further questioned what is new from this framework in relation to others such as NIST cybersecurity framework? Chapter 5 which is framework design explained in detail the motivation behind the design of the NBCF and how different it is from the existing frameworks such as NIST. For instance, although the NBCF has incorporated all the six components from the NIST framework, an additional component 7 of “compliance” was added to it which is not part of NIST.

Figure 5.5 highlights that a total of 90% of the reviewers indicated that the framework is either very relevant and/or relevant in the mitigation of cybersecurity challenges in Namibia banking institutions while only 10% of the reviewers indicated that it is least relevant. With these responses, it’s a clear indication that the framework will be relevant if implemented in the Namibian financial sector, however the framework will need continuous enhancements and improvements in light of the 10% views of the respondents.

6. Please select the appropriate choice from the following options. To what extent do you agree that the framework is relevant in the mitigation of cybersecurity challenges in Namibia banking institutions?

10 responses

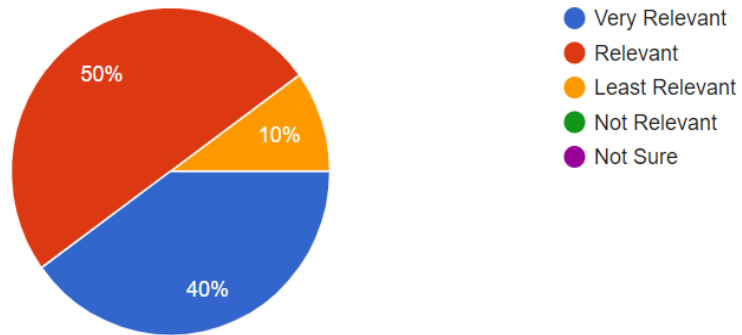


Figure 5.5 Framework relevance

To demonstrate the applicability of the framework as highlighted in figure 5.6, a total of 50% of the reviewers agreed that the framework is very applicable in Namibia's banking institutions, while 40% of the reviewers indicated that the framework is applicable. On the other hand, 10% indicated that the framework is somewhat applicable in Namibian banking institutions. Therefore, this is a clear indication that the framework will be of value and use in the Namibian banking sector and can still be improved further.

7. To what extent do you agree that the framework is applicable in Namibia banking institutions?

10 responses

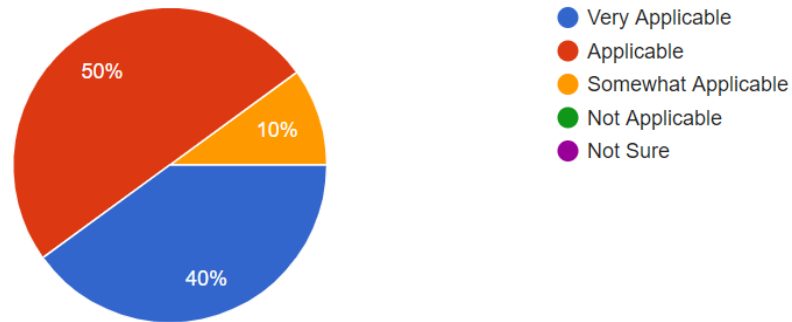


Figure 5.6 Framework applicability

Figure 5.7 highlights that 20% of the reviewers agree that the framework is very suitable in improving the banking institution's cyber resilience, the ability to respond, withstand and recover from cyber incidents and attacks while 50% of the reviewers indicated that the framework is suitable. On the other hand, 30% indicated that they agree that the framework is somewhat suitable in improving the banking institutions' cyber resilience. Therefore, the overall review of the suitability of the framework is considered to be highly applicable.

8. To what extent do you agree that the framework is suitable in improving the banking institutions' cyber resilience (the ability to respond, withstand and recover from cyber incidents and attacks)?

10 responses

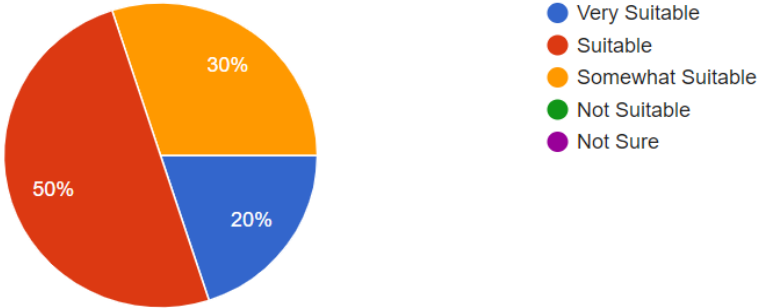


Figure 5.7 Framework suitability

The significance of the NBCF was evaluated and the results are presented in Figure 5.8. A total of 20% of the reviewers agreed that the framework is very significant, while the other 60% agreed that the framework is indeed significant. On the other hand, 20% of the reviewers highlighted that the framework is somewhat significant. There is therefore a clear indication that the framework will be of significant use in the financial sector if implemented by the banks. The framework will however need continuous enhancement and improvements in light of the 20% concern views of the respondents.

9. To what extent do you agree that the framework is significant in Namibia banking institutions?

10 responses

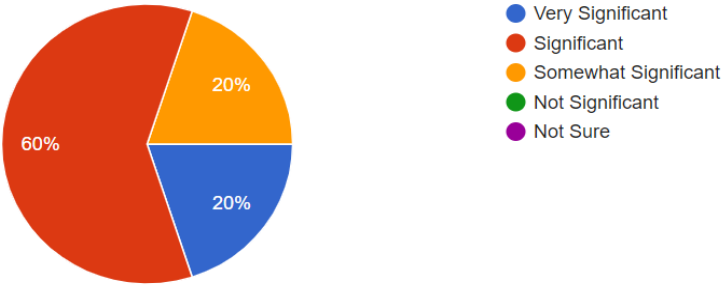


Figure 5.8 Framework significance

Figure 5.9 is a representation results of whether the framework is understandable or not. A total of 10% of the reviewers indicated that the framework is very understandable while 70% of the reviewers indicated that the framework is understandable. On the other hand, 20% of the reviewers differed and indicated that the framework is somewhat understandable. This is a good indication that the framework context and details are easy to understand as none of the reviewers disagreed to that. Therefore, the framework's components will not be changed.

10. To what extent do you agree that the framework is understandable?

10 responses

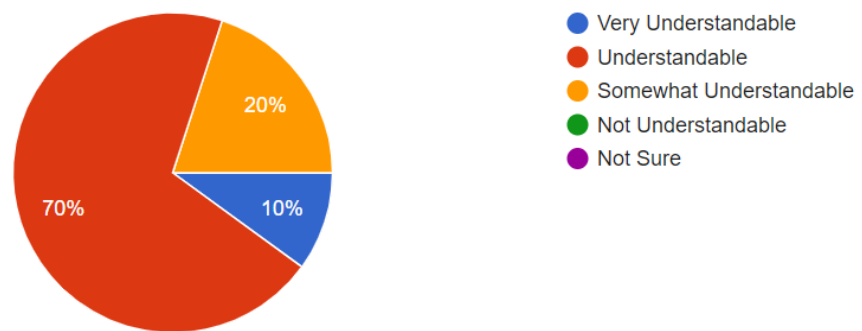


Figure 5.9 Framework understandability

The clarity of the interconnectedness of the framework components were evaluated as indicated in figure 5.10. A total of 20% of the reviewers strongly agree that the framework components are logically connected to each other and thus they provide cyber resilience to the bank. A total of 80% of the reviewers also agreed that components are logically connected. The evaluation shows that all the reviewers agreed that the framework components are logically connected to each other hence the relationships and framework components will be maintained.

11. To what extent do you agree that the components are logically connected to each other and thus provide cyber resilience to the bank?

10 responses

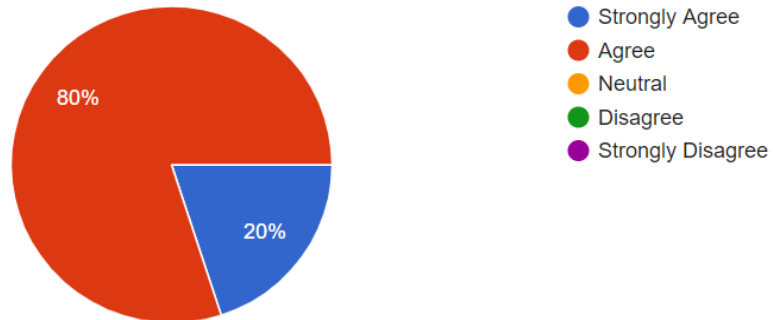


Figure 5.10 Framework components connection

The framework adoptability was also evaluated as indicated in figure 5.11. A total of 20% of the reviewers strongly agreed that the framework can be adopted by organisations aiming at enhancing their ability to detect and monitor cybersecurity events, threats and risks in order to improve their cyber resilience, while 40% agreed. On the other note, 40% of the reviewers were neutral on the framework adoptability. This is therefore a clear indication that although the framework will be of utmost importance in enhancing the bank's ability to detect and monitor cybersecurity events, threats and risks, the framework needs to be well communicated on the steps and procedures for adoptability. This will be addressed in section 5.8.

12. To what extent do you agree that the framework can be adopted by organisations aiming at enhancing their ability to detect and monitor cybersecurity events, threats and risks in order to improve their cyber resilience?

10 responses

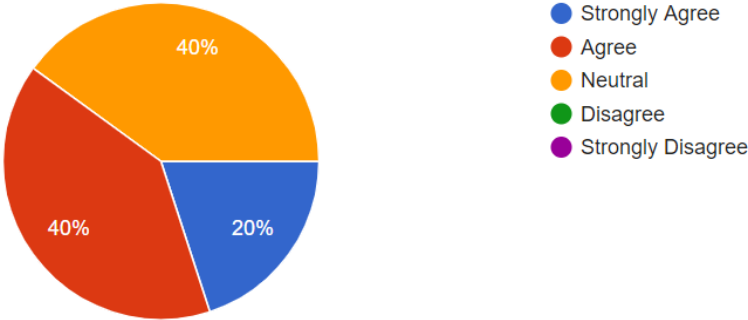


Figure 5.11 Framework adoptability

Table 5.20 presents reviewers' comments on framework suitability, applicability, relevance and significance.

Table 5.20 Reviewer’s responses on framework suitability, applicability, relevance and significance

Reviewer	To what extent do you agree that the framework is relevant in the mitigation of cybersecurity challenges in Namibia banking institutions?	To what extent do you agree that the framework is applicable in Namibia banking institutions?	To what extent do you agree that the framework is suitable in improving the banking institution’s cyber resilience (the ability to respond, withstand and recover from cyber incidents and attacks)?	To what extent do you agree that the framework is significant in Namibia banking institutions?	To what extent do you agree that the framework is understandable?	To what extent do you agree that the components are logically connected to each other and thus provide cyber resilience to the bank?	To what extent do you agree that the framework can be adopted by organisations aiming at enhancing their ability to detect and monitor cybersecurity events, threats and risks in order to improve their cyber resilience?
Reviewer 1	Very Relevant	Very Applicable	Very Suitable	Very Significant	Understandable	Agree	Strongly Agree
Reviewer 2	Very Relevant	Very Applicable	Suitable	Significant	Understandable	Agree	Agree
Reviewer 3	Very Relevant	Very Applicable	Very Suitable	Very Significant	Very Understandable	Strongly Agree	Strongly Agree
Reviewer 4	Very Relevant	Very Applicable	Suitable	Significant	Understandable	Strongly Agree	Agree
Reviewer 5	Relevant	Applicable	Suitable	Significant	Understandable	Agree	Agree
Reviewer 6	Relevant	Applicable	Suitable	Somewhat Significant	Understandable	Agree	Agree
Reviewer 7	Least Relevant	Somewhat Applicable	Somewhat Suitable	Somewhat Significant	Understandable	Agree	Neutral

Reviewer 8	Relevant	Applicable	Suitable	Significant	Understandable	Agree	Neutral
Reviewer 9	Relevant	Applicable	Somewhat Suitable	Significant	Somewhat Understandable	Agree	Neutral
Reviewer 10	Relevant	Applicable	Somewhat Suitable	Significant	Somewhat Understandable	Agree	Neutral

Table 5.20 presents the response of reviewers regarding the suitability, applicability, relevance and significance of the framework. Firstly, 90% of the reviewers indicated that the framework is relevant in the mitigation of cybersecurity challenges in Namibian banking institutions. All the reviewers believed that the framework is applicable in Namibian banking institutions. Furthermore, 60% of the reviewers indicated that the framework is suitable in improving the banking institution’s cyber resilience (the ability to respond, withstand and recover from cyber incidents and attacks). Most of the reviewers had almost similar opinions when asked about the significance of the framework; 80% agreed that the framework is significant in Namibian banking institutions. When asked if the framework was understandable, 80% of the reviewers indicated that the framework is understandable/very understandable. Reviewers were also asked to rate the framework in terms of usability; of which all of them indicated that the framework is usable/very usable. In the questionnaire, 60% stated that the framework can be adopted by organisations aiming at enhancing their ability to detect and monitor cybersecurity events, threats and risks in order to improve their cyber resilience as indicated in Table 5.20. Based on the feedback obtained from reviewers, the framework is considered to be suitable, applicable, relevant and significant in combating cybersecurity issues. However, there are notable suggested changes proposed by the reviewers as given in table 5.22.

III. Comments and Recommendations

A total of 40% highlighted that they would recommend changes to the framework, while 60% recommended no changes. These proposed changes are presented in table 5.21.

Figure 5.12 presents responses on the framework changes.

13. Would you recommend any change to the framework components?

10 responses

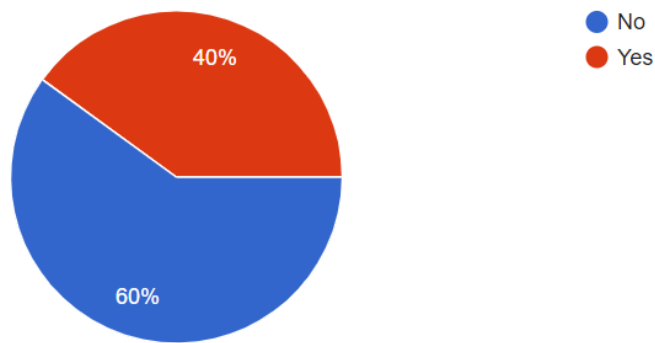


Figure 5.12 Framework components changes

Table 5.21 Reviewers' framework component changes and recommendations

Reviewer	Would you recommend any change to the framework components?	If Yes, please specify the changes per component listed below:	Proposed Change
Reviewer 1	No		
Reviewer 2	No		
Reviewer 3	No		No changes needed the framework is well designed.
Reviewer 4	No		
Reviewer 5	Yes	Protection	Add training of Cybersecurity experts under protection, since they too play a pivotal role in cyber resilience.

Reviewer 6	No		
Reviewer 7	Yes	Identification	Approach needs to take strategic goals and objectives into consideration.
Reviewer 8	No		
Reviewer 9	No		
Reviewer 10	Yes		I need to understand the framework better first or what is new to the others to be able to provide a better answer on the applicability.

The following changes were implemented as recommended by the reviewers

1. Adding training of cybersecurity experts to the protection component: Reviewers suggested that not only user awareness training is needed, but cybersecurity experts need to be trained as cybersecurity technologies and issues are ever evolving. The researcher also deemed it a valid recommendation as it is suitable to add training of cybersecurity experts to the protection component.
2. Organisational strategic goals and objectives were incorporated into the identification component.

A total of 40% highlighted that they would recommend changes to the relationships between the framework components, while 60% recommended no changes. These 40% proposed changes which are presented in table 5.22.

Figure 5.13 presents the proposed components relationship changes of the framework.

14. Would you recommend any change to the relationships between the framework components?

10 responses

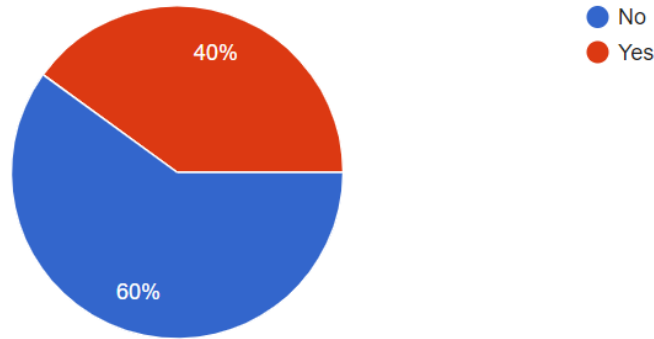


Figure 5.13 Framework components' relationship changes

Table 5.22 Reviewers' recommendations

Reviewer	Would you recommend any change to the relationships between the framework components?	If Yes, please specify the changes per component listed below:	Proposed Change
Reviewer 1	No		
Reviewer 2	No		
Reviewer 3	No		
Reviewer 4	No		

Reviewer 5	Yes	Recovery	Data Security under protection needs to be linked to data recovery.
Reviewer 6	No		
Reviewer 7	Yes	Protection	Compliance with standards plays a key role within the protection of assets.
Reviewer 8	No		
Reviewer 9	No		
Reviewer 10	Yes		We will have to discuss this as you must first take me through it and explain it better.

The following changes were implemented as suggested by the reviewers:

1. Data security under protection was linked to data recovery. The framework was refined and a relationship was created between protection and recovery components.
2. Compliance with standards plays a key role within the protection of assets. It should therefore be noted that the protection component initially had been linked (there had been a relationship) with the compliance component.

Question: Do you have any other comments?

Table 5.23 presents reviewers' final comments

Table 5.23 Reviewers' final comments

Reviewer	Would you recommend any change to the proposed framework? Addition of or removal of components?	Do you have any other comments?	Researcher's take on the comments
Reviewer 1	No changes. The framework is comprehensive.	The framework will be useful in enhancing cybersecurity within the banking sector in Namibia.	Agreed.

Reviewer 2		The framework components are understandable and relevant, but the controls and best practices beneath those components will determine its success.	Agreed. It should however be noted that the controls are clearly articulated on the framework design - refer to figure 5.2 - Proposed Namibia Banking Cybersecurity Framework (NBCF) and table 5.24 - overview of the Namibia Banking Cybersecurity Framework were the activities and/or controls are clearly defined.
Reviewer 3	No changes required	Well-designed framework.	Agreed.
Reviewer 4	The proposed framework will be a great tool to adopt locally in addition to available international frameworks. A continuous evaluation of the implementation of it will be worth noting and will provide a true reflection of its effectiveness.	No further comments.	
Reviewer 5	Add training of cybersecurity experts and link recovery and protection together	None.	
Reviewer 6			
Reviewer 7	The framework should take into consideration core regulations such as BID30.	<p>In the current form, the framework serves to be a consolidation of frameworks and would not add value to organizations that have their own defined frameworks, standards and policies. Due to the fact that within the design of most organisational frameworks, standards and policies, the review and adaptation of international standards and framework are key components.</p> <p>In addition, the framework would be difficult to implement for roughly half the banking industry in Namibia due to limited staff dedicated to</p>	<p>Researcher did not adopt these comments because firstly, these international standards and frameworks differ from country to country. One of the reasons this is so is because of environmental and situational differences. It should be noted that Namibia is different from other countries.</p> <p>Furthermore, literature clearly revealed that the focus of the majority of the international framework studies contain only few cybersecurity features such as security policies, procedure, best practice, standards, and guidelines, security program,</p>

		information security within the banks outside the big 4.	monitoring and compliance, user awareness, education and training, risk management and assessment processes and no attention was given to the other essential features such as human factors and cybersecurity simulations. Some gaps exist in them and their conceptualisation of cyber risks in the banking sector hampers their adaptation in developing countries like Namibia.
Reviewer 8	N/A	N/A	
Reviewer 9	N/A	N/A	
Reviewer 10	Yes. Let's discuss it.	I am just concerned at what is new. The headings are similar to NIST CSF but you need to convince me first that your framework would be better than the NIST framework or ISF CF for example.	What is new is that, although the NBCF has incorporated all the six components from the NIST framework and other frameworks, an additional component 7 of "compliance" was added to it which is not part of NIST. A gap was identified in the existing frameworks, that the compliance component was missing as banking institutions are subjected to comply with a number of industry, national and international laws and regulations. Failure to adhere to some of these laws and regulations may result in serious negative consequences for the business operations.

5.6.5 Conclusion

The evaluation was aimed at verifying and confirming the validity and reliability of the NBCF framework. The weighting process measurements were contained in five evaluation criteria

namely relevance, applicability, usability, adaptability and understandability. Based on the feedback obtained from the expert reviewers, the framework is considered to be highly relevant, applicable, usable and understandable in combating cybersecurity issues in the Namibian banking sector.

As a result of the evaluation, the following changes were effected:

1. Adding training of cybersecurity experts to the protection component.
2. Data security under protection was linked to data recovery.
3. Organisational strategic goals and objectives were incorporated into the identification component. Under the identification component, one of the controls is identifying risk mitigation strategies. It was therefore refined by clearly stipulating “identifying risk mitigation strategies which are aligned with the organisational strategic goals and objectives”.

5.7 Refinement of the Framework

The purpose of the evaluation completed in section 5.6 aimed at aiding the refinement of the framework. This is the reason why the reviewers’ comments and recommendations were noted and incorporated in the framework enhancement. Table 5.24 presents the reviewers’ final comments.

Table 5.24 Reviewers’ final comments

Reviewer	Suggestions/Comments	Improvements Made
Reviewer 5	Detection of cybersecurity attacks as presented in the framework is more technical and excludes trained experts. Not all attacks can be detected by technological solutions. There also needs to be a component on Security Expert training. This can be done with the addition of another component or it	Added training of cybersecurity experts to the protection component

	being integrated into the existing components, especially under Protection and Response.	
Reviewer 7	The influence of strategic goals and objectives of an organisation are not taken into consideration with identifying critical assets.	Organisations' strategic goals and objectives were incorporated into the identification component. Under the identification component, one of the controls is identifying risk mitigation strategies. It was therefore refined by clearly stipulating "identifying risk mitigation strategies which are aligned with the organisational strategic goals and objectives". Refer to table 5.25.
Reviewer 5	Data security under protection needs to be linked to Data recovery.	Data security under protection was linked to data recovery.

Figure 5.14 presents the refined NBCF.

The refined Namibia Banking Cybersecurity Framework (NBCF)

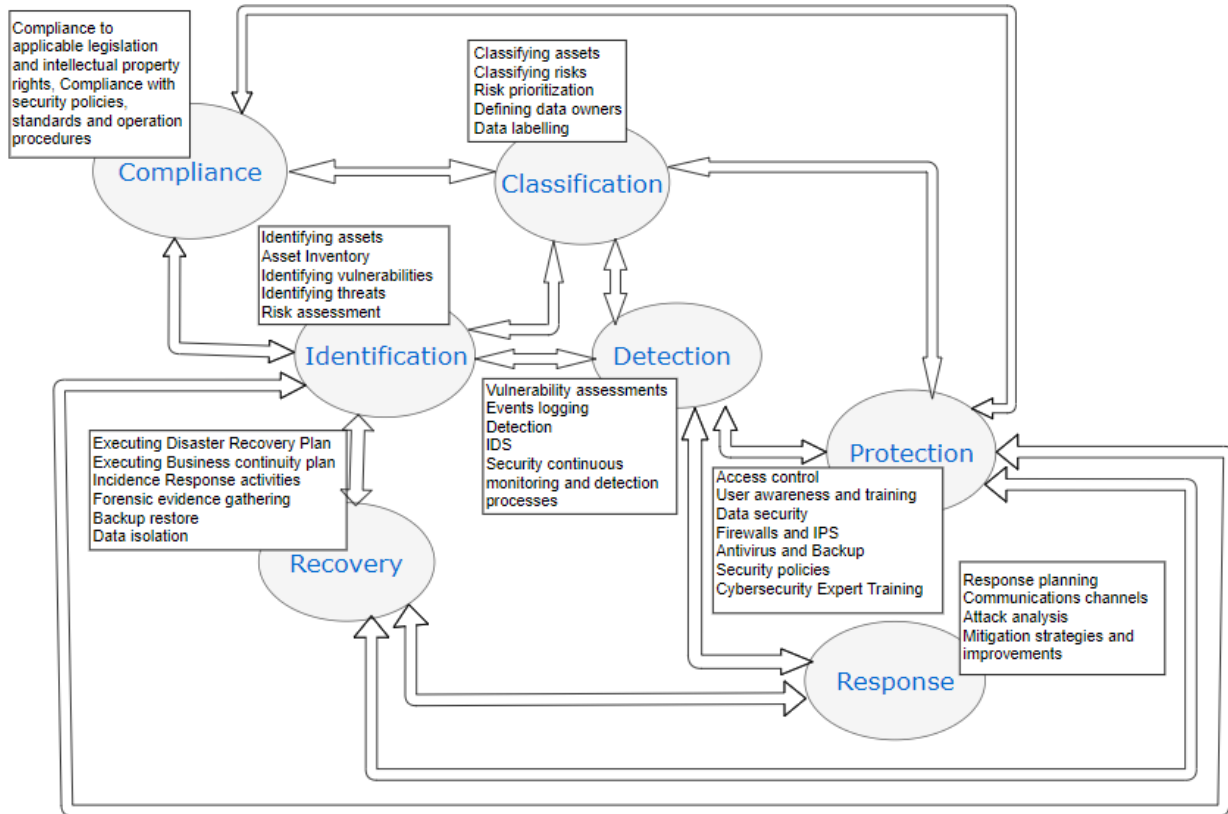


Figure 5.14 The Namibia Banking Cybersecurity Framework (NBCF)

The listed changes as recommended by the reviewers were effected as follows:

1. Added training of cybersecurity experts to the protection component.
2. Data security under protection was linked to data recovery.
3. Organisations' strategic goals and objectives were incorporated into the identification component.

5.8 Communication

According to Hevner et al. (2004), Design-science must be presented both to technology-oriented as well as management-oriented audiences. Technology-oriented audiences need sufficient detail to enable the described artifact to be constructed (implemented) and used within an appropriate organizational context. Management-oriented audiences need sufficient detail to determine if the organizational resources should be committed to constructing (or purchasing) and using the artifact within their specific organizational context” (p.90). The NBCF will be communicated through raising the framework awareness to banking institutions in Namibia and providing guidelines on how to apply the framework to their environments. Also, it will be published in scholarly publications. By communicating the proposed NBCF, practitioners will take advantage of the benefits offered by the framework and it will provide researchers with a knowledge base for additional extensions and evaluation.

The proposed NBCF comprises of seven components namely identification, classification, protection, detection, response, recovery and compliance as shown in table 5.8. In each category, there are security domains, security objectives and activities which provide an overview of the whole framework.

Table 5.25 communicates the framework components, security objectives and activities.

Table 5.25 Overview of the Namibia Banking Cybersecurity Framework

	IDENTIFICATION	CLASSIFICATION	PROTECTION	DETECTION	RESPONSE	RECOVERY	COMPLIANCE
Sub-components	<ul style="list-style-type: none"> Asset management 	<ul style="list-style-type: none"> Information asset classification and handling 	<ul style="list-style-type: none"> Access control Physical and environmental security Human resource security Cryptography Operations security Communications security 	<ul style="list-style-type: none"> Monitoring Vulnerability assessment 	<ul style="list-style-type: none"> Information security incident management 	<ul style="list-style-type: none"> Information security aspects of business continuity management 	<ul style="list-style-type: none"> Information security policies Organization of information security
Security Objectives	<ul style="list-style-type: none"> To identify all organisations information assets, potential risk and define the appropriate level of protection in order to achieve the strategic goals and objectives of the organisation. 	<ul style="list-style-type: none"> To ensure that information assets are subject to an appropriate level of defence 	<ul style="list-style-type: none"> To ensure that organisational information can be viewed and accessed by authorised and intended people only To ensure that information processing facilities are secure To identify security best practice 	<ul style="list-style-type: none"> To assess security risks and threat they pose. To mitigate risks to prevent security incidents and compliance failures To review operational security practices 	<ul style="list-style-type: none"> To ensure consistent and effective approaches to the lifecycle of incidents and responses 	<ul style="list-style-type: none"> To create an effective system to manage business disruptions and to be able to contain the impact of a potential cyber security incident 	<ul style="list-style-type: none"> To comply with relevant laws and regulations, legal and contractual requirements, best practice and ethical conduct
Activities	This involves identifying key business areas, all inventory of assets, defining asset ownership and assessing potential risk, risk management	Activities include measuring information assets, value, criticality and sensitivity, information labelling and information handling procedures	User security awareness, training of cybersecurity experts, controlling user and devices access to networks and network services, defining user access	Tracking and logging user, device activities, network and systems scans to discover loopholes	Creating procedure, assigning of roles reporting information security weaknesses, incidents and breaches	Planning information security continuity, disaster recovery plans, equipment and procedures	Compliance to Information Security policies, applicable legislation, and intellectual property rights. Compliance regulation of cryptographic use controls

	strategies and risk mitigation strategies which are aligned with the organisational strategic goals and objectives.		rights, removal or adjustment of access rights, implementing operating system access control, information access control				Compliance with security policies and standards and operational procedures
--	---	--	--	--	--	--	--

5.9 Chapter Summary

This chapter discussed the design process of the proposed NBCF framework in sections 5.4 and 5.5. It presented the design in its six steps in sections 5.2 to 5.8. The chapter's main discussion was formed by the development of the framework in section 5.4 and evaluation in section 5.6. Major components of the framework are identification, classification, protection, detection, response, recovery and compliance. The identification component serves to identify critical functions, information assets and corresponding risks which influence strategic goals and objectives of the organisation. This allows an organisation to focus and prioritise its activities in accordance with its risk management strategy, asset value and business requirements. The classification component's purpose is to ensure that all information assets in physical or digital form are classified accordingly. Information should be classified in compliance to legal, regulatory requirements, or organisational policies. The protection component is meant for application of security measures and controls to safeguards information assets. Both logical and physical security measures can be applied. These include: identity management and access control, user awareness and training. The detection component's main function is to identify incidents and potential occurrences of cybersecurity events. This enables timely discovery of cyber security events and potential attacks. An incident response plan should be implemented to address a suspected data breaches. An incident response plan guides how an organisation will react in the event of a security breach. The response component is meant to minimise damage, decrease disaster recovery time, and mitigate breach-related expense. An organisation should be able to contain the impact of potential cybersecurity incidents. The recovery component is meant for the restoration of any services disrupted by a cybersecurity incident. In this case, an organisation should be able to mitigate an attack with a meaningful and practiced incident response plan. The compliance component is aimed at ensuring compliance or adherence to a minimum of the security-related requirements such as legal requirements or security policies and standards, and technical compliance. The components are defined in more detail in section 5.4.1. After its design, the framework accomplishes the goal of supporting efforts to deal with complex and emerging cybersecurity issues in the banking sector in order to strengthen their cybersecurity postures. The NBCF framework was evaluated by experts in the cybersecurity field, and they

confirmed the relevance, usability and efficiency of the framework in achieving the research objectives. The next chapter is the last chapter which presents the future considerations and conclusion of the research study.

CHAPTER SIX: FUTURE CONSIDERATIONS AND CONCLUSION

6.1 Overview

The first five chapters conferred the research problem and research objectives, literature review, research methodology, data analysis, as well as the Namibia Banking Cybersecurity Framework design and evaluation. As cyber threats continue to emerge, cybersecurity has become a great concern in the banking sector. This has been exacerbated by the foundation of banking which lies in nurturing trust and credibility. Banks therefore need to be on their guard more than most businesses as they have high public-facing products and services. This is due to their key role in settlement and payment systems, as well as the high volume of sensitive customer information that they process. The most common cybercrime-related threats include data breaches, customer identity theft, fraudulent money transfers and unplanned system downtime. In this research, a cybersecurity framework was developed for the Namibian banking sector; its fitness for implementation was evaluated and it proved to be of great significance.

This chapter presents the research summary, reflection and lessons learnt, research limitations, future directions and research conclusion.

6.2 Research Contributions

The first objective of the study was to assess the various patterns of cybercrimes associated with online transactions in the Namibian banking institutions' cyberspace. An understanding of the latest trends of cybersecurity threats in banking institutions was also achieved in section 2.3. It was discovered through the literature review that credit card frauds are the number one vector of cybercrimes and this has been exacerbated by the advancements in e-commerce payment technology (section 2.4). The banking sector mostly suffers from phishing attacks, ransomware, insider attacks and DDoS as presented in sections 2.2 and 2.3.

The second objective was to evaluate the existing cybersecurity frameworks. Many financial institutions are putting in place national policies or international frameworks to strengthen their cybersecurity postures. These frameworks provide best practices to oversee or provide guidance on cybersecurity issues. In this research, an evaluation of the top 5 international cybersecurity frameworks assessing the strength and weaknesses and gaps associated with these frameworks was done; the NIST cybersecurity framework, the CPMI-IOSCO cybersecurity framework, ISO/IEC 27001:2013 framework, CIS, and the framework for the Governance of Information Security in the Banking System as indicated in section 2.7. The analysis concluded that cybersecurity standards and frameworks differ from country to country. Therefore, evaluation helps in proposing improvement elements within these frameworks hence why the NIST cybersecurity framework, ISO/IEC27001: 2013 and the Framework for the Governance of Information Security in Banking System frameworks were chosen for further application in this study.

The third objective was to develop a cybersecurity framework to guide banking institutions in managing online financial transactions. In order to design the proposed framework for Namibia, the researcher evaluated the existing cybersecurity frameworks and standards through a literature review and identified gaps within them such as corporate governance, ethical conduct, trust, and the auditor security programme as indicated in section 2.7. In addition, semi-structured interviews carried out with banking staff also helped to identify gaps such as data protection and privacy, human factor such as soft skills, Principle of Least Privilege (POLP), public knowledge on information security practices, aspect of disaster recovery documentation and cyber breach simulations within these frameworks and standards applied within the Namibian banking processes. Thus, the proposed NBCF framework can help to combat cybersecurity issues identified in the Namibian financial sector.

This study serves the basis to continue to expand and update the locally recognised cyber security body of knowledge. This framework supports efforts to deal with complex and emerging cybersecurity issues in the banking sector by providing a baseline of security objectives and activities to be implemented. The framework draws on standard methodologies used to assess

various types of cyber risks and can be easily applied at the individual and organisational level as implementation guidelines are provided.

6.3 Reflection and Lessons Learnt

I have gained some incomparable knowledge on cybersecurity, specifically the various international cybersecurity frameworks such as NIST cybersecurity framework, The CPMI-IOSCO cybersecurity framework, ISO/IEC 27001:2013 Standards on Information Security Management System, CIS and a Framework for the Governance of Information Security in the Banking System. I have learnt about several research design processes (such as design science and engineering science) in an attempt to identify the one suitable for this study hence the use of the design science research methodology. I have also gained exposure on the different data collection methods such as interviews and questionnaires as well as exposure to the qualitative data analysis methods which helped me with data analysis. This research study has also provided me with the opportunity to explore my academic abilities and I have also acquired new research skills such as being creative and coming up with solutions to problems.

Lessons learnt are as listed here:

- The latest global cybersecurity threat trends in the banking sector as presented in chapter 2 section 2.3, which are mobile and web banking security; the use of third parties; compliance; insider vulnerabilities; large user population; gaps in technology; phishing attacks; ransomware; insider attacks and DDoS.
- Current cybersecurity gaps and weaknesses in the Namibian banking sector, which are insider threats, phishing attacks, web banking security and user awareness.
- The status of the Namibian banking sector with regards to cybersecurity is behind in adopting international trends and policies and Namibia does not have the technical nor financial abilities to deal with cyber threats.
- The responsibility to assess cybersecurity vulnerabilities and implement security measures to mitigate cyber risk is for everyone.
- Cybersecurity threats can be mitigated by managing the human factor.

6.4 Research Limitations

The main limitation was that the study was not carried out on all 11 licensed banks in Namibia due to lack of responses from the banks as only 6 banks were responsive. The other constraints that have been identified in this research study were limitations of time, and resources (banks staff) which were not fully available; the framework was not pilot tested on any bank thus it was not possible to produce a complete walkthrough of the fully implemented framework. Due to COVID-19 it became so difficult to perform a complete walkthrough as most staff were working in isolation thus hindering a walkthrough. Due to these constraints it was therefore not possible to completely evaluate the operating and effectiveness of the framework in the real world.

6.5 Future Considerations

The recommendations for further study include similar research in other sectors of Namibia with consideration for use of a different design methodology and conceptual framework for research diversity. This study has contributed to the literature; however, additional research is warranted as reported in the study's findings. Topics were found in this study that serve as relevant issues in the cybersecurity discipline and the IT skills. Therefore, the researcher recommends the following:

- Perform studies using a cyber-threat lens. This perspective of an organisation's infrastructure may reveal a better understanding of crucial indicators such as offender intent and motivation, target selection and exploitation choices, and perceptions into cyber defense tradecraft and effectiveness of guardianship.
- Research how conventional vulnerability based cybersecurity approaches could be enhanced to help enable cybersecurity resiliency.
- Use data science tradecraft to provide a better understanding of critical infrastructure borne of the convergence of IT and Operational Technology (OT) that presents a complex cybersecurity challenge.
- Focus upon cybersecurity training strategies through collaborative teaming with the compliance and training programs.

6.6 Research Conclusion

The main research goal of this study was to develop a cybersecurity framework for the banking sector of Namibia. This was achieved by creating and evaluating the proposed NBCF framework for the Namibian banking sector. Chapter 5 presented the proposed framework and its suitability in the Namibian context. This study also reviewed and documented the available evidence on cyber-attacks in the banking institutions. Additionally, the analysis showed that cyber-risk is an emerging threat for all financial institutions. The study provides a roadmap to deal with cybersecurity issues in the Namibian banking sector and it contributes to the cybersecurity body of knowledge in the banking sector.

The study findings indicate that there could be positive change in strategies used by IT and compliance professionals to mitigate cyber threats and promote cyber resilience in the Namibian banking institutions. Improvements in the protection of their critical assets may strengthen confidence, trust and reputation in the community and society. A catastrophic failure in critical infrastructure, as a result of cyber-attacks or natural disaster, has been reported in the news media with the potential to impact national security and public safety. The study findings identified key factors necessary for an improved cybersecurity strategy for protecting banks and the developed Namibia Banking Cybersecurity Framework (NBCF) will also go a long way to building cyber resilience. The increased occurrence of successful cyber-attacks has resulted in the disruption of key utility services and loss of personal financial data. Luo (2016) found that concerns have increased within communities, and society in general, on the ability of the government and banking industry to protect its citizens and customers. This study provided an exploration and contextual analysis of strategies in cybersecurity and developed a framework for the banking institutions which will provide a high-level, strategic view of an organisation's cybersecurity risk management and will be of assistance to IT and compliance professionals in these banking institutions. Successful protection of critical infrastructure benefits banking institutions and customers by ensuring that key services are sustained during crisis events. This success also contributes to improving and enhancing the IT body of knowledge by protecting sensitive industry and customer's data that enables the continued flexibility in using modern

technologies. In addition, the study findings may help improve employee behaviours towards cybersecurity and compliance. Lastly, once the banking institutions adopt and implement the framework, future research should be performed to find out about its flexibility, implications on BoN, relevant cyber laws and governance.

References

- Acharya, A. S., Prakash, A., Saxena, P., & Nigam, A. (2013). Sampling: Why and how of it. *Indian Journal of Medical Specialities*, 4(2), 330–333.
- Acocella, I. (2012). The focus groups in social research: advantages and disadvantages. *Quality & Quantity*, 46(4), 1125–1136.
- Alshenqeeti, H. (2014). Interviewing as a data collection method: A critical review. *English Linguistics Research*, 3(1), 39–45.
- Bank of Namibia Annual Report, (2017).
<https://www.bon.com.na/CMSTemplates/Bon/Files/bon.com.na/92/92d106b2-a920-4168-be80-ec1645e42e95.pdf>
- Bank of Namibia Annual Report, (2019).
<https://www.bon.com.na/CMSTemplates/Bon/Files/bon.com.na/3a/3af2b4ce-c0f2-4e99-9d68-dc64a7c1ecb4.pdf>
- Bank of Namibia, *BID-30 Information Security*. Retrieved from
<https://www.bon.com.na/CMSTemplates/Bon/Files/bon.com.na/be/be1d4b35-dffc-4c0d-85a1-6faf52e3d836.pdf>
- Bank Windhoek. (2021). *Bank Windhoek releases new Mobile App*.
<https://www.bankwindhoek.com.na/Pages/News/Bank-Windhoek-releases-new-Mobile-App.aspx>
- Bekhet, A. K., & Zauszniewski, J. A. (2012). Methodological triangulation: An approach to understanding data. *Nurse Researcher*, 20(2), 1-11.
- Bhasin, M. L. (2015). *Menace of frauds in the Indian banking industry: An empirical study*. *Australian Journal of Business and Management Research*, 4(12), 1-13.
- Blessing, L., Chakrabarti, A., & Wallace, K. (1995). A design research methodology. In *Proc. International Conference on Engineering Design 1995 ICED* (pp. 50–55).
- Borrion, H., & Yuryna Connolly, L. (2020). *Your money or your business: Decision-making processes in ransomware attacks. Incomplete*
- Bouveret, A. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment*.

International Monetary Fund.

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum*, 41(5), 545-547.

Center for Internet Security. (2018). *CIS controls*. East Greenbush, NY: CIS. <https://www.cisecurity.org/>

Chochliouros, I. P., Spiliopoulou, A. S., Stephanakis, I. M., Arvanitosis, D. N., Sfakianakis, E., Belesioti, M., ... Mitsopoulou, N. (2015). Security and Protection of Critical Infrastructures: A Conceptual and Regulatory Overview for Network and Information Security in the European Framework, also focusing upon the Cloud Perspective. In *Proceedings of the 16th International Conference on Engineering Applications of Neural Networks (INNS)* (p. 28).

Collis, J., & Hussey, R. (2013). *Business research: A practical guide for undergraduate and postgraduate students*. Macmillan International Higher Education.

Committee on Payments and Market Infrastructure (CPMI). (2016). *Board of the International Organization of Securities Commissions: Guidance on cyber resilience for financial market infrastructures*. Bank for International settlements. CPMI-IOSCO.

Creswell, J. W., & Poth, C. N. (2017). *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications.

Crisanto, J.C., & Prenio J. (2017). *Regulatory approaches to enhance bank's cyber-security frameworks*. Financial Stability Institute insights on policy implementation No 2: Bank for international settlements

De Hoyos, M., & Barnes, S. (2012). *Analysing interview data*. Warwick Institute for Employment Research. [Http://Www2. Warwick. Ac. Uk/Fac/Cross_fac/Socialsciencesdtc/Coretrainingmodules/Quals/Analysing_interview_data_1_-_w6. Pdf.](http://www2.warwick.ac.uk/Fac/Cross_fac/Socialsciencesdtc/Coretrainingmodules/Quals/Analysing_interview_data_1_-_w6.Pdf)

Doody, O., & Noonan, M. (2013). Preparing and conducting interviews to collect data. *Nurse researcher*, 20(5), 28-32.

Dutton, W., Goldsmith, M., Saunders, J., Varese, F., & Von Solms, B. (2019). *Cybersecurity capacity review*. Ministry of Information and Communication Technology.

- Ellis, T. J., & Levy, Y. (2010). A guide for novice researchers: Design and development research methods. In *Proceedings of Informing Science & IT Education Conference (InSITE)*, 10, pp. 107–118).
- Erastus, L., Jere, N., & Shava, F. B. (2017). A security model for Namibian Government Services. In *IST-Africa Week Conference (IST-Africa), 2017* (pp. 1–11).
- Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1–4.
- Goldkuhl, G. (2012). Pragmatism vs interpretivism in qualitative information systems research. *European Journal of Information Systems*, 21(2), 135–146.
- Government of the Republic of Namibia. (1996). *Manual of guidelines for common minimum standards of protective security measures for Government Ministries/Public Offices and Agencies of the Republic of Namibia*. Office of the President.
- Gray, D. E. (2014). *Doing research in the real world. [electronic resource]*. (S. Jai, Ed.) (3rd ed.). Sage.
- Harambee Prosperity Plan (2016). *Harambee Prosperity Plan*
<http://www.gov.na/documents/10181/264466/HPP+page+70-71.pdf/bc958f46-8f06-4c48-9307-773f242c9338>
- Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 75–105.
- IBM X-Force Threat Intelligence Index (n.d.) *IBM x-force threat intelligence index*.
<https://www.ibm.com/security/data-breach/threat-intelligence>.
- Iec, I. S. O. (2013). *Information technology - Security techniques - Information security management systems - requirements*. <https://www.iso.org/standard/54534.html>
- International Organization for Standardization [ISO] 31000:2009 (2009). *Risk management - Principles and guidelines/ISO Guide 73:2009*. Risk Management-Vocabulary.
- Internet World Stats. (2020). *Usage and population statistics*.
<https://www.internetworldstats.com/stats1.htm>
- Jain, N., & Khan, V. (2018). Credit card fraud detection using recurrent attributes. *People*, 5(2), 43-47.

- Jazri, H., & Jat, D. S. (2016). A quick cybersecurity wellness evaluation framework for critical organizations. In *ICT in Business Industry & Government (ICTBIG), International Conference on* (pp. 1–5).
- Kaspersky Lab (n.d.). *Kaspersky Lab financial cyber threats report*.
https://usa.kaspersky.com/about/press-releases/2019_kaspersky-lab-financial-cyberthreats-report
- Khan, S. R. (2018). Implication of cyber warfare on the financial sector. An exploratory study. *International Journal of Cyber-Security and Digital Forensics*, 7(1), 31–38.
- Kothari, C. R., & Garg, G. (2014). *Research methodology and techniques*. New Age International Publications.
- Kritzinger, E., & Von Solms, S. H. (2012). A framework for cyber security in Africa. *Journal of Information Assurance & Cybersecurity*, 2012, 1.
- Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice*, 16(4), 473–475.
- Li, J. X. (2017). Cyber crime and legal countermeasures: A historical analysis. *International Journal of Criminal Justice Sciences*, 12(2), 196–207.
- Luo, X. (2016). Security protection to industrial control system based on defense-in[1]depth strategy. *WIT Transactions on Engineering Sciences*, 113, 19-27.
 doi:10.2495/IWAMA150031
- Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research: A guide to design and implementation*. John Wiley & Sons.
- MOHAMMED, D. (2018). Cybersecurity compliance in the financial sector. *The Journal of Internet Banking and Commerce*, 20(1), 1–11.
- Muganda, N. (2010). *Applied business and management research: Exploring the principles and practices of research within the context of Africa*.
<http://repository.tukenya.ac.ke/handle/123456789/1185>
- MTC (2016). *MTC annual report 2016*. <http://www.mtc.com.na/sites/annual-reports/2016/pdf/MTC-Annual-Report-2016.pdf>
- National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical*

- infrastructure cybersecurity*. <https://csrc.nist.gov/publications/detail/white-paper/2018/04/16/cybersecurity-framework-v11/final>
- Olivier, F. (2017, June 2). Cybercrime in Namibia. *The Namibian*. <https://www.namibian.com.na/165301/archive-read/Cybercrime-in-Namibia>
- Order, E. (2013). 13636. US Government Presidential Executive Order 13636 - Improving Critical Infrastructure Cybersecurity. Whitehouse,US. <http://www.whitehouse.gov>
- Ormston, R., Spencer, L., Barnard, M., & Snape, D. (2014). The foundations of qualitative research. *Qualitative Research Practice: A Guide for Social Science Students and Researchers*, 2, 52–55.
- Peppers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3), 45–77.
- Rahman, A., & Abedin, M. J. (2021). The Fourth Industrial Revolution and private commercial banks: The good, bad and ugly. *International Journal of Organizational Analysis*. <https://doi.org/10.1108/IJOA-05-2020-2218>
- Saunders, M., Lewis, P., & Thornhill, A. (2016). *Research methods for business students* (7th ed.). Edinburgh Gate: Pearson Education Limited.
- Security Intelligence (2016). Security Intelligence. <https://securityintelligence.com/five-cybersecurity-challenges-facing-financial-services-organizations-today/>
- Shirodkar, N., Mandrekar, P., Mandrekar, R. S., Sakhalkar, R., Kumar, K. M. C., & Aswale, S. (2020). Credit card fraud detection techniques--A survey. In *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)* (pp. 1–7).
- Telecom Namibia (2017). *Telecom Namibia 2016/2017 annual report*. <http://www.telecom.na/downloads/reports/2016-17/Annual%20Report%202016-2017.pdf>
- Teoh, C. S., Mahmood, A. K., & Dzazali, S. (2017). Is NIST CSF applicable for developing nations? A case study on Government Sector in Malaysia. In *PACIS* (p. 101). <http://aisel.aisnet.org/pacis2017/101>

- Thanh, N. C., & Thanh, T. T. (2015). The interconnection between interpretivist paradigm and qualitative methods in education. *American Journal of Educational Science*, 1(2), 24–27.
- Ula, M., Ismail, Z., & Sidek, Z. M. (2011). A framework for the governance of information security in banking system. *Journal of Information Assurance & Cyber Security*, 2011, 1–12.
- Umanailo, M. C. B., Fachruddin, I., Mayasari, D., Kurniawan, R., Agustin, D. N., Ganefwati, R., ... others. (2019). Cybercrime case as impact development of communication technology that troubling society. *Int. J. Sci. Technol. Res*, 8(9), 1224–1228.
- Verschuren, P., Doorewaard, H., & Mellion, M. J. (2010). *Designing a research project*. Eleven International publishing house.
- Wagner, C., Kawulich, B., & Garner, M. (2012). *Doing social research: A global context*. McGraw-Hill Higher Education.
- Wall, D. S. (2015). *The Internet as a conduit for criminal activity. Information technology and the criminal justice system*, Pattavina, A., ed, 77-98.
- World Economic Forum. (2020). How to protect yourself from cyberattacks when working from home during COVID-19. <https://www.weforum.org/agenda/2020/03/covid-19-cyberattacks-working-from-home/>
- World Economic Forum. (2020). *Why cybersecurity matters more than ever during the coronavirus pandemic*. <https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity/>
- Yaseen, Q. (2016). *Insider threat in banking systems*. 10.4018/978-1-5225-0864-9.ch013.
- Yildirim & Varol. (2019). *A Research on Security Vulnerabilities in Online and Mobile Banking* doi - 10.1109/ISDFS.2019.8757495
- ZDNet (2018). Bank web apps are the "most vulnerable" to getting hacked, new research says. <https://www.zdnet.com/article/bank-sites-and-web-apps-are-most-vulnerable-to-hackers/>
- ZDNet (2020). COVID-19 blamed for 238% surge in cyberattacks against banks. <https://www.zdnet.com/article/covid-19-blamed-for-238-surge-in-cyberattacks-against-banks/>

Appendix A: Interview Questions



13 Jackson Kaujeua Street
Private Bag 13388
Windhoek
NAMIBIA

T: +264 61 207 2481
F: +264 61 207 9481
E: di@nust.na
W: www.nust.na

17 February 2022

Dear Sir/Madam,

RE: DEVELOPING A CYBERSECURITY FRAMEWORK FOR THE BANKING SECTOR OF NAMIBIA

I am a student, pursuing a Master degree in Informatics at the Namibia University of Science & Technology (NUST). I am currently conducting research titled “**Developing a cybersecurity framework for the financial sector of Namibia**”. Since there is a rapid spread of new advanced digital technologies and the rise of new disruptive threats, most organisations are digitally transforming their business models and processes. With society's increasing dependence on Information Technology (IT), the consequences of computer crime can be extremely grave. We, therefore, see this research as critical and is likely to contribute to the improvement of banking sector’s preparedness to the cybersecurity related threats and risks.

We would like to seek your feedback on the semi-structured interview questions to help us **assess the various patterns of cybercrimes associated with online transactions and evaluate existing cybersecurity frameworks**. Please be assured that this information is sought for research purposes only and your responses will be strictly confidential. No individual’s responses will be identified as such and the identity of persons responding will not be published or released to anyone. All information will be used for academic purposes only.

For the purpose of this study, I will be recording the interview session. Before I start with the interview, I would like the respondent to please sign the acceptance of the interview voice recording (consent letter).

QUESTIONS RELATED TO CYBER SECURITY PRACTICES IN THE BANK

1. Did your organisation experience any cyber-attacks over the past years?
2. What were the various types of cyber-attacks experienced? How many of the attacks were successful and managed to compromise the environment?
3. Are these types of cyber-attacks associated with online transactions?
4. What do you think is the main vulnerability for cyber-attacks experienced in your organisation?
5. How did you handle/contain the types of cyber events mentioned above?
6. Are your organisation's personnel properly trained and understand the nature of cyber security and their role in protecting the organisation's information asset?
7. What are the local and international information/cyber security standards and frameworks have you adopted in your organisation?
8. Have you fully adopted each standard/framework's functions, categories and/or elements?
9. Do you think there are some important aspects and elements that the international standards and frameworks did not cover? What are those elements and why do you believe they were supposed to be part of the standards/framework?
10. What value would these elements add to the standard/framework?
11. Do you have any policies, procedures and programs that support the information security function which helps the function in identifying cyber security risks, strengths, and weaknesses?

Evaluation Questionnaire of the Proposed Namibia Banking Cybersecurity Framework (NBCF)

Dear Participants,

This questionnaire serves to evaluate the relevancy and usability of the Namibia Banking Cybersecurity Framework (NBCF) in the Namibian banking institutions. It also further evaluates how the banking institutions can adopt the framework to their facilities in order to enhance their cybersecurity posture.

The framework has seven components combined together to provide the following objectives:

1. Identify critical information assets inventory and business functions.
2. Detect cybersecurity attacks in the banking sector in a timely manner.
3. Protect human resources and information system assets of the banking sector.
4. Effectively respond to detected cybersecurity attacks.
5. Recover from cybersecurity attacks.
6. Comply with organisational, national, industry, international policies, regulations and laws.

Information collected will be used to improve the framework design. The resulting framework will contribute to the guidelines on how the Namibian financial institutions can securely build cyber resiliency, manage their cyber risks and strategies and also help in implementing an appropriate level of rigor for their cybersecurity programs. Your responses are crucial in informing the design of the framework.

The study is conducted by Eva-Lisa Tuwilika Nawa, a Master of Informatics student, under the supervision of Prof. Fungai Bhunu Shava and Dr. Mercy Chitauro from the Namibia University of Science and Technology (NUST).

All your responses will be treated in a confidential manner; hence you are invited to provide genuine responses. No personal information will be collected from you. All the collected information will be used for the purposes of this study only and when reporting no information which can identify you will be disclosed, where verbatim quotes are used a pseudo reference will be used such as participant 1, 2, and so on. The questionnaire will take about 10-20 minutes of your time.

For any further information, kindly contact me on +264814532622 or evalisanawa4@gmail.com

Thank you for your time and contribution.

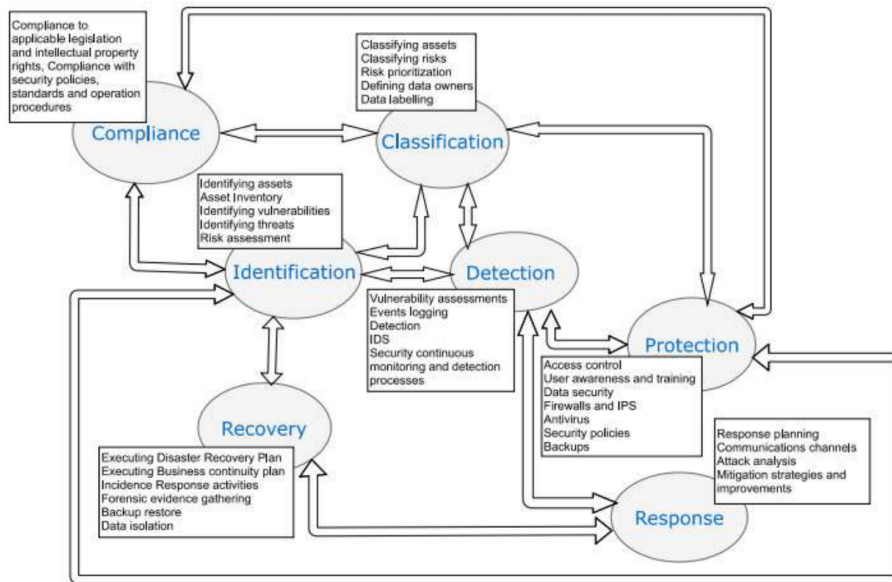
* Required

Description of the proposed Namibia Banking Cybersecurity Framework (NBCF)

The proposed framework comprises of seven components with each serving a specific function. The seven components are identification, protection, detection, response, recovery and compliance. Each component serves a specific area of security domain with corresponding security elements. The proposed NBCF provide cybersecurity risk management strategies to both technical and managerial audiences. It advocates for cyber resilience with the main focus on cybersecurity risk management. By using the framework, financial institutions will be able to build cyber resiliency, where systems and operations are designed to detect cyber threats and respond to and recover from cyber events to minimise business disruption and financial losses.

The framework will apply to all banking institutions in Namibia. It will be a coordinated management of technology, intelligence, and business operations to efficiently manage the bank's information assets, reputation and protect critical assets from external and internal threats through technical and non-technical measures. Please refer to the figure below of the proposed framework.

Proposed Namibia Banking Cybersecurity Framework (NBCF)



Demographic Information

This section aims to understand your area of work/study and your experience in that field.

1. Educational qualification *

Mark only one oval.

- First Degree
- Honours Degree
- Master Degree
- PhD
- Other: _____

2. Relevant Professional Certifications (Choose all applicable) *

Mark only one oval.

- CISSP
- CISM
- CISA
- CRISC
- CGEIT
- PMP
- CompTIA Security+
- Other: _____

3. Please indicate your role in your organisation (choose one) *

Mark only one oval.

- Chief Information Security Officer
- Head of Information Security
- Information Security Manager/Specialist
- ICT Manager
- Information Security Engineer
- Network Security Specialist
- IT Risk Specialist/Analyst
- Other: _____

4. Please specify your IT Risk or Information Security years of experience *

Mark only one oval.

- 0-5 years
- 6-10 years
- 11-20 years
- More than 20 years

Framework Evaluation

This section aims at evaluating the framework.

5. Please answer each question in this section by selecting a single choice per question (row) *

Mark only one oval per row.

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
To what extent do you agree that the framework will support identification of critical information assets inventory and business functions?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
To what extent do you agree that the framework will help in detecting cybersecurity attacks in the banking sector in a timely manner?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
To what extent do you agree that the framework will support in protecting human resources of the banking sector?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
To what extent do you agree that the framework will support in protecting information system assets of the banking sector?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
To what extent do you agree that the framework will help banking institutions in effectively responding to detected cybersecurity attacks?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
To what extent do you agree that the framework will help banking institutions in recovering from cybersecurity attacks?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

If you have any comments for question 5, please elaborate.

6. Please select the appropriate choice from the following options. To what extent do you agree that the framework is relevant in the mitigation of cybersecurity challenges in Namibia banking institutions? *

Mark only one oval.

- Very Relevant
- Relevant
- Least Relevant
- Not Relevant
- Not Sure

7. To what extent do you agree that the framework is applicable in Namibia banking institutions? *

Mark only one oval.

- Very Applicable
- Applicable
- Somewhat Applicable
- Not Applicable
- Not Sure

8. To what extent do you agree that the framework is suitable in improving the banking institutions' cyber resilience (the ability to respond, withstand and recover from cyber incidents and attacks)? *

Mark only one oval.

- Very Suitable
- Suitable
- Somewhat Suitable
- Not Suitable
- Not Sure

9. To what extent do you agree that the framework is significant in Namibia banking institutions? *

Mark only one oval.

- Very Significant
- Significant
- Somewhat Significant
- Not Significant
- Not Sure

10. To what extent do you agree that the framework is understandable? *

Mark only one oval.

- Very Understandable
- Understandable
- Somewhat Understandable
- Not Understandable
- Not Sure

11. To what extent do you agree that the components are logically connected to each other and thus provide cyber resilience to the bank? *

Mark only one oval.

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

12. To what extent do you agree that the framework can be adopted by organisations aiming at enhancing their ability to detect and monitor cybersecurity events, threats and risks in order to improve their cyber resilience? *

Mark only one oval.

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

Comments and
Recommendations

This section focuses on the framework comments and recommendations.

13. Would you recommend any change to the framework components? *

Mark only one oval.

- No
- Yes

If Yes, please specify the changes per component listed below:

Mark only one oval.

- Identification
- Classification
- Protection
- Detection
- Response
- Recovery
- Compliance

14. Would you recommend any change to the relationships between the framework components? *

Mark only one oval.

- No
- Yes

If Yes, please specify the changes per component listed below:

Mark only one oval.

- Identification
- Classification
- Protection
- Detection
- Response
- Recovery
- Compliance

15. Would you recommend any change to the proposed framework? Addition of or removal of components?

16. Do you have any other comments?

This content is neither created nor endorsed by Google.

Google Forms

Appendix C: Ethical Clearance



FACULTY RESEARCH ETHICS COMMITTEE (F-REC)
DECISION/FEEDBACK ON RESEARCH PROPOSAL

Dear Ms: Eva-Lisa Nawa

Research Topic: **Developing a cyber-security framework for the financial sector of Namibia**

Supervisor (if applicable): **Dr Fungai Bhunu Shava**

Qualification registered for (if applicable): **MASTER OF INFORMATICS**

(Reference number of application: **FACULTY RESEARCH ETHICS COMMITTEE REGISTRATION NUMBER: F-REC-16/2019**)

Re: Ethical screening application No: **F-REC-16/2019**

The Faculty of **Computing and informatics** Ethics Screening Committee of the Namibia University of Science and Technology reviewed your application for the above-mentioned research. The research as set out in the application has been:

Approved

(indicate with an X, and N/A if not applicable and proceed)

We would like to point out that you, as researcher, are obliged to maintain the ethical integrity of your research, adhere to the ethical guidelines of NUST, and remain within the scope of your research proposal and supporting evidence as submitted to the F-REC. Should any aspect of your research change from the information as presented to the F-REC, which could have an effect on the possibility of harm to any research subject, you are under the obligation to report it immediately to your supervisor or F-REC as applicable in writing. Should there be any uncertainty in this regard, you have to consult with the F-REC.

We wish you success with your research, and trust that it will make a positive contribution to the quest for knowledge at NUST.

Any ethical issues that need to be highlighted?	Why are these issues important?	What must/could be done to minimise the ethical risk?
No	N/A	N/A

Recommendation: The application is approved: Recommendations of FCI/F-REC, communicated to you on the 10th of October 2019, were addressed to the satisfaction of the Chairperson.

Sincerely,

Dr Fungai BHUNU SHAVA

Chair: Faculty Ethics Screening Committee

Tel: +264-61-207-2510

CC: Co-supervisor: Mrs Mercy Chitauro



Appendix D: Sample – Data Collection Permission Letter



**NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY**
Faculty of Computing and Informatics

Department of Informatics

13 Jackson Kaujeua Street
Private Bag 13388
Windhoek
NAMIBIA

T: +264 61 207 2481
F: +264 61 207 9481
E: di@nust.na
W: www.nust.na

Trustco Bank Namibia Limited
PO Box 11363
Windhoek

12 November 2019

Dear Sir/Madam,

RE: SEEKING PERMISSION TO COLLECT DATA FROM TRUSTCO BANK NAMIBIA LIMITED EMPLOYEES, THE FINDINGS WILL INFORM THE DEVELOPMENT OF A CYBER SECURITY FRAMEWORK FOR THE FINANCIAL SECTOR OF NAMIBIA

My name is Eva-Lisa Nawa and I am a Master of Informatics student (student number: 214062414) at the Namibia University of Science and Technology (NUST) under the supervision of Dr Fungai Bhunu Shava. This course is research based and the research I wish to conduct for my Master's thesis is entitled, "Developing a cyber security framework for the financial sector of Namibia". I am hereby seeking your permission to allow the involvement of your employees in this research. The research will involve the employees taking part in the interviews which are designed to assess the various patterns of cybercrimes associated with online transactions and evaluate the existing cyber security frameworks. The results will be used as the basis to develop a sustainable cyber security framework that will guide the adoption of cyber security best practices in the Namibian banking sector. Your bank has valuable contribution to the banking sector in Namibia hence why we have chosen to engage with you.

Information about the Research

The main objective is to develop a cyber-security framework to guide financial institutions in safeguarding online transactions of financial data between banks and customers.

To achieve the main objective, the following sub objectives are proposed:

- Assess the various patterns of cybercrimes associated with online transactions in the Namibian financial institutions' cyberspace.
- Evaluate the existing cyber-security frameworks.
- Develop a cyber-security framework to guide financial institutions in managing online financial transactions.

Data collection Process

Data collection procedure will carefully follow the authorisation given in the research consent letter.



**NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY**

Faculty of Computing and Informatics

Department of Informatics

13 Jackson Kaujeua Street
Private Bag 13388
Windhoek
NAMIBIA

T: +264 61 207 2481
F: +264 61 207 9481
E: di@nust.na
W: www.nust.na

Participation and Confidentiality

For the research participants to make a free and informed consent they will be provided with full details on what the research is about, its purpose, how long the study will take, research procedures and the expected benefits of the research study. Complete confidentiality and ethical use of information provided shall be maintained throughout; and consent shall be sought for your approval of the use of the information.

Participants have the right to refuse or withdraw any time from partaking in the interviews. You do not have to take part in this study if you do not wish to do so. All data collected from this study will be kept confidential and will be used for academic purposes only. No personal information will be collected and the data will be recorded generically, where need be a pseudo identifier will be used in order to maintain privacy. Please note that any information gathered up to the point of withdrawal might be utilized inside the study.

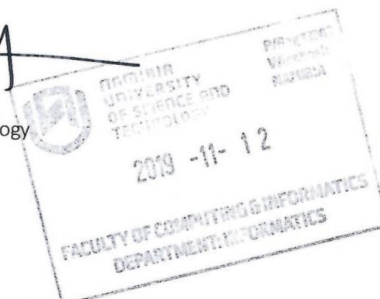
The findings from this study will be shared more broadly through thesis publications and conference publications, and will be treated as confidential and your bank name will not be mentioned as such. The resulting framework which will be developed to adopt cyber security best practices in the financial sector will be brought to the bank for accuracy verification and evaluation.

Your permission to conduct this study will be greatly appreciated.

Further Questions and Contact Details

For more information or for any questions about the research, please do not hesitate to contact me or my supervisor. Details are as follows:

- a) Dr Fungai Bhunu Shava 
Associate Dean: Research and Innovation
Namibia University of Science and Technology
Faculty of Computing and Informatics
Department of Computer Science
Email: fshava@nust.na
- b) Ms Eva-Lisa Nawa
Student: Namibia University of Science and Technology
Department of Informatics
Windhoek; Namibia
Cell number: +264 81 453 2622
Email: evalisanawa4@gmail.com



Appendix E: Participants' Consent Form



NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY
Faculty of Computing and Informatics
Department of Informatics

13 Jackson Kaujeua Street
Private Bag 13388
Windhoek
NAMIBIA

T: +264 61 207 2481
F: +264 61 207 9481
E: di@nust.na
W: www.nust.na

Dear Participant,

My name is Eva-Lisa Nawa, a student at the Namibia University of Science and Technology (NUST), pursuing a Master degree in Informatics (Cybersecurity). I am conducting a research study titled **"Developing a cybersecurity framework for the financial sector of Namibia"**.

With the current era of advanced digital technologies and the rise of new disruptive threats, banks are significantly vulnerable to cybercrimes as they offer high public facing products and services. The purpose of this study is to shed light on how banks can enhance their processes and procedures in order to mitigate online transactions' cyber threats. Specifically, the research will focus on assessing the various patterns of cybercrimes associated with online transactions and evaluating the existing cyber security frameworks. This study is critical and likely to contribute to the improvement of the cyber maturity of the banking sector of Namibia. I therefore humbly request for your participation in this study.

Responses to the interviews will be completely anonymous. Thus, personal information will **NOT** be recorded and only aggregate data will be used in reports. Please note that for the purpose of this study, the interview session will be recorded and confidentiality will be strictly maintained. Note that your participation in this study is entirely voluntary.

I have read the above informed consent, the nature and benefit of the study and:

Hereby agree

Do not agree

Participant role: Group COO Infrastructure

Signature of participant: Date: 5/02/2020




NAMIBIA UNIVERSITY
OF SCIENCE AND TECHNOLOGY
Faculty of Computing and Informatics
Department of Informatics

13 Jackson Kaujeua Street
Private Bag 13388
Windhoek
NAMIBIA

T: +264 61 207 2481
F: +264 61 207 9481
E: di@nust.na
W: www.nust.na

I acknowledge that I have explained the nature and purpose of the study. Thank you for your consent, any enquiries regarding this study can be directed to me at email: evalisanawa4@gmail.com.

Signature of interviewer:  Date: 05/02/2020

Appendix F: Language Editor's Report

ACET Consultancy
Anenyasha Communication, Editing and Training
Box 50453 Bachbrecht, Windhoek, Namibia
Cell: +264814218613
Email: mlambons@yahoo.co.uk / nelsonmlambo@icloud.com

18 August 2021

To whom it may concern

LANGUAGE EDITING – EVA-LISA TUWILIKA NAWA

This letter serves to confirm that a **Master of Informatics** thesis entitled ***DEVELOPING A CYBERSECURITY FRAMEWORK FOR THE BANKING SECTOR OF NAMIBIA*** by Eva-Lisa Tuwilika Nawa was submitted to me for language editing.

The thesis was professionally edited and track changes and suggestions were made in the document. The research content or the author's intentions were not altered during the editing process and the author has the authority to accept or reject my suggestions.

Yours faithfully



DR NELSON MLAMBO
PhD in English
M.A. in Intercultural Communication
M.A. in English
B. A. Special Honours in English – First class
B. A. English & Linguistics