AFRICA UNIVERSITY

(A United Methodist-Related Institution)

An Assessment of Cyber Risk Management Effectiveness in Zimbabwe's Financial Sector: A Case of National Building Society (NBS).

BY

CHARLES GWINYAYI MAPSWAYI

A DISSERTATION/THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF EXECUTIVE MASTERS IN BUSINESS ADMINISTATION AT THE COLLEGE OF BUSINESS AND MANAGEMENT SCIENCES

2025

Abstract

The growing prevalence of cyber threats in the global financial sector has made cybersecurity a central component of institutional resilience and risk governance. This study assessed the effectiveness of cyber risk management strategies employed by the National Building Society (NBS) in Zimbabwe, with a focus on identifying key vulnerabilities, evaluating existing control mechanisms and proposing enhancements to strengthen cyber resilience. The research was guided by four objectives: to establish and categorize the major cyber threats and system vulnerabilities affecting NBS's operations in the last 10 years, to evaluate the effectiveness of existing cyber risk management controls and policies at NBS in reducing cyber incidents in the past 10 years 3, to assess the likelihood and impact of identified cyber risks on NBS's operational, financial and reputational performance in the last 10 years and to recommend improved strategies for managing these risks. The study adopted a mixed-methods case study design combining quantitative and qualitative approaches to obtain a comprehensive understanding of the phenomenon. A total of 186 employees were targeted, with 132 valid responses obtained through structured questionnaires and follow-up interviews. Quantitative data was analysed using descriptive statistics, correlation and regression analyses through the latest SPSS version, while qualitative data was subjected to thematic analysis. The findings revealed that although NBS has implemented several cybersecurity measures including incident response planning, employee awareness training and business continuity systems, significant gaps persist in policy communication, phishing prevention and external collaboration with cybersecurity partners. The descriptive results showed that the mean perception of cyber risk management effectiveness was moderate ($M = 3.49$), indicating room for improvement. Correlation analysis established a significant negative relationship between the effectiveness of cyber risk strategies and exposure to cyber risks ($r = -0.474$, $p < 0.01$), suggesting that stronger cybersecurity practices directly reduce perceived vulnerability. Regression results indicated that 22.5% of the variance in exposure to cyber risks could be explained by the effectiveness of NBS's cyber risk management strategies. Qualitative insights highlighted human factors, outdated legacy systems and limited technological investment as persistent challenges to achieving cyber resilience. The study concludes that while NBS demonstrates commendable progress toward developing a cybersecurity framework, its effectiveness remains constrained by inadequate employee engagement, limited automation and inconsistent risk assessment processes. It recommended adopting a zero-trust security model, strengthening staff training, increasing collaboration with regulatory and law enforcement bodies and integrating cybersecurity governance into enterprise risk management. The study contributed to the understanding of cyber risk management within developing economies and offered practical insights for policymakers and financial institutions seeking to enhance cybersecurity effectiveness in Zimbabwe's financial sector.

Key Words: Cyber Risk, Risk Management, Strategies, Effectiveness, Data Security, Breach.

Declaration

I declare that this dissertation is my original work except where sources have been cited and acknowledged. The work has never been submitted, nor will it ever be submitted to another university for the award of a degree.

Charles G Mapswayi	
Student's Full Name	Student's Signature
Prof (Dr) Yogesh Kumar Awashthi	
Main Supervisor's Full Name	Main Supervisor's Signature

Copyright

Acknowledgments

I am humbly appreciative of my supervisor Prof. Yogesh Kumar Awasthi for his guidance and support during crafting this dissertation. My appreciation also goes to faculty and the administration for creating a conducive learning environment and all the support provided. I greatly appreciate my classmates who have been in this journey for the past one and a half years and not forgetting Prof Murairwa for the providing all the learning resources in this program.

Dedication

I dedicate this thesis to my wife, Lisa Motsi, for her unwavering support, encouragement and dedication to see me pull through. I also want to dedicate this to my special children, Tafara, Tanatswa and Elora Mapswayi for giving me room to focus and work on this project with the utmost attention.

List of Acronyms and Abbreviations

AI	Artificial Intelligence
BAZ	Bankers Association of Zimbabwe
DDoS	Distributed Denial of Service
DFRWS	Digital Forensics Research Workshop
DLP	Data Loss Prevention
IoT	Internet of Things
IT	Information Technology
NBS	National Building Society
POTRAZ	Postal and Telecommunications Regulatory Authority of Zimbabwe
RBZ	Reserve Bank of Zimbabwe
SPSS	Statistical Package for the Social Sciences
TAM	Technology Acceptance Model
ZICT	Zimbabwe Information and Communication Technologies
AI/ML	Artificial Intelligence / Machine Learning

List of Tables

List of Figures

Definition of Key Terms

Cyber Risk - The potential for financial loss, disruption, or reputational damage resulting from a failure of information technology systems or from unauthorized access, cyber-attacks, or data breaches within an organization's digital infrastructure.

Cyber Risk Management -The systematic process of identifying, assessing, and mitigating cyber threats to minimize their impact on organizational operations, assets, and data integrity.

Cybersecurity - The practice of protecting computer systems, networks, and data from digital attacks, unauthorized access, and damage through preventive and corrective technological and procedural measures.

Legacy Systems - Older computer systems or applications still in use within an organization, which may lack modern security features and increase vulnerability to cyber threats.

Incident Response - The organized approach an organization follows to address and manage the aftermath of a cybersecurity breach or attack, aimed at limiting damage and reducing recovery time and costs.

Effectiveness -The degree to which objectives are achieved and intended outcomes are realized. In this study, it refers to how successfully the National Building Society's (NBS) cyber risk management strategies mitigate cyber threats and protect critical information assets**.**

Exposure to Cyber Risk - The extent to which an organization's systems, data, or processes are vulnerable to cyber-attacks, potentially leading to operational, financial, or reputational harm.

Fraud Triangle Theory - A criminological model suggesting that fraud arises when three elements coexist: pressure, opportunity, and rationalization — relevant to insider threats in cybersecurity**.**

National Building Society (NBS) - A Zimbabwean financial institution providing mortgage and banking services; the case study organization examined in this research for cyber risk management effectiveness.

Phishing -A cyber-attack method in which attackers impersonate legitimate entities to deceive individuals into revealing sensitive information such as passwords or financial data.

Ransomware - A type of malicious software that encrypts a victim's files or systems, demanding payment (ransom) for the decryption key to restore access.

Risk Management - The coordinated process of identifying, analysing, evaluating, and responding to potential risks that could affect an organization's objectives. It involves developing and implementing strategies to minimize or control the probability and/or impact of adverse events.

Technology Acceptance Model (TAM) - A theoretical framework explaining how users come to accept and use technology, often based on perceived usefulness and ease of use.

Table of Contents

CHAPTER 1: INTRODUCTION

1.1 Introduction

The increasing threat of cyber risks within the financial services sector presents significant challenges to institutions worldwide, including the National Building Society (NBS). Despite the deployment of cybersecurity measures, vulnerabilities remain, indicating potential weaknesses in current strategies. This study evaluates the effectiveness of cyber risk management approaches used by NBS to mitigate these growing threats. It identifies gaps and proposes enhancements to strengthen NBS's cybersecurity defences. This chapter provides the study's context, problem statement, objectives, research questions, assumptions/hypotheses, significance, scope and limitations. The chapter ends with a Chapter summary.

1.2 Background to the Study

Globally, the financial sector is grappling with a surge in cybercrime. Cybercrime's worldwide cost is estimated to be around US$1 trillion annually (Thomson Reuters Accelus, 2018). This includes financial losses for businesses and individuals, as well as broader consequences for national security and economic stability. The rise in cybercrime stems from rapid digital transformation, increased internet access and the growing sophistication of cybercriminals exploiting technological weaknesses. Cybersecurity Ventures (2021) projects that global cybercrime costs will exceed $10.5 trillion annually by 2025, highlighting the urgent need for robust defense strategies. Cyber threats extend beyond financial losses, posing risks to critical infrastructure and public safety. Prominent incidents, such as the 2013 distributed denial-of-service

(DDoS) attacks on major U.S. banks, exposed vulnerabilities in essential services and underscored the potential impact of inadequate cybersecurity (Roberta, 2013).

As organizations become more reliant on interconnected systems, they are increasingly vulnerable to coordinated attacks with far-reaching consequences. The World Economic Forum (2020) emphasizes that improving cybersecurity resilience is vital for protecting economies and maintaining public trust in digital transactions. A Feedzai report (2020) indicates that cyber risks significantly contribute to fraud within the financial sector. Across the African continent, cybercriminal activity is on the rise. The Financial Fraud Action Africa Report (2022) indicates a 20% increase in losses from African cybercrimes between 2018 and 2021. This increase is linked to the growing use of digital payment systems and the absence of strong cybersecurity measures. In South Africa, the South African Banking Risk Information Centre (SABRIC) (2021) reported a 3% increase in credit card cloning between 2017 and 2021.

In Zimbabwe, cybercrime is a growing concern. Card cloning incidents jumped from 41 in 2018 to 160 in 2019 (ZICT Report, 2020). In July 2024, a ransomware attack on ZB Bank (ZICT Report, 2024) resulted in the theft and release of sensitive data, causing system disruptions. The Bankers Association of Zimbabwe (BAZ) has also reported increased hacking attempts on other banks (ZICT Report, 2024). These incidents highlight the increasing cyber threats facing the Zimbabwean banking sector. This study focuses on NBS due to its unique position as a building society in Zimbabwe. Unlike commercial banks, NBS primarily focuses on providing affordable housing finance. This specialization may result in a different risk profile and cybersecurity needs compared to larger, diversified financial institutions. Understanding these specific needs is crucial for developing effective cyber risk

management strategies tailored to NBS. This research aims to develop effective cyber risk management strategies for financial institutions in Zimbabwe, with a specific focus on NBS.

1.3 Statement of the Problem

Cybercrime is a growing threat both globally and in Zimbabwe. The UK estimates annual cybercrime costs at £27 billion, while global cybercrime reaches approximately US$1 trillion (Thomson Reuters Accelus, 2018). The increase in card cloning incidents and the ransomware attack on ZB Bank in July 2024 highlight the urgent need for effective cybersecurity measures in Zimbabwe. While banks are working to improve their cybersecurity, current strategies often fall short due to an over-reliance on reactive measures. Many strategies prioritize responding to incidents instead of preventing them. Inadequate employee training makes employees susceptible to social engineering and phishing attacks. Limited investment in advanced technologies hinders the adoption of AI-driven threat detection and prevention systems. Gaps in regulatory compliance, along with inconsistent adherence to cybersecurity standards, further exacerbate these vulnerabilities. This study investigates the effectiveness of cyber risk management strategies used by NBS to determine whether additional or corrective strategies are needed to mitigate cyber threats effectively.

1.3 Research Objectives

1. To establish and categorize the major cyber threats and system vulnerabilities affecting NBS's operations in the last 10 years.
2. To evaluate the effectiveness of existing cyber risk management controls and policies at NBS in reducing cyber incidents in the past 10 years.

3. To assess the likelihood and impact of identified cyber risks on NBS's operational, financial and reputational performance in the last 10 years. of cyber risks encountered by the NBS.
4. To develop practical, institution-specific recommendations for strengthening cyber risk management at NBS, aligned international best practices.

1.4 Research Questions

1. What were the major cyber threats and vulnerabilities affecting NBS's operations in the last 10 years?
2. How effective are NBS's current cyber risk management strategies and controls in preventing, detecting and responding to cyber threats during the period?
3. What is the impact and likelihood of cyber risks on NBS's operational continuity, financial stability and customer trust NBS?
4. What context-appropriate improvements can be proposed to enhance NBS's cyber risk management framework in compliance with best international practices?

1.5 Significance of the Study

This section highlights the importance of the research, both practically and theoretically. This research offers practical strategies for Zimbabwean financial institutions, particularly the NBS, to strengthen their cyber risk management practices. Given the increasing sophistication of cyber threats targeting the financial sector in Zimbabwe, as evidenced by the ZB Financial Holdings ransomware attack in 2024 and the rise in card cloning incidents (ZICT Report, 2020), this study is relevant. The analysis will provide NBS management and other financial institutions with insights

into the specific challenges they face, enabling them to develop targeted and effective cybersecurity measures. The findings will contribute to improved cybersecurity practices, enhanced customer trust of the financial system in Zimbabwe.

Furthermore, the research will contribute to the broader understanding of cyber risk management in developing economies, where resources and infrastructure may differ significantly from developed nations. Readers, including industry professionals, policymakers and academics, will gain valuable insights into the challenges and opportunities associated with cyber risk management in the Zimbabwean financial sector. This knowledge can inform decision-making, promote a deeper understanding of the importance of cybersecurity in maintaining consumer trust and ensure safe and efficient banking practices. For the researcher, this study represents an opportunity to contribute to a vital area of knowledge within cybersecurity and banking in Zimbabwe. The research findings can also serve as a springboard for future investigations, leading to further academic publications and contributions to the field.

This study contributes to theoretical frameworks related to technology adoption (e.g., Technology Acceptance Model, Routine Activity Theory and Fraud Triangle Theory). It will challenge current models and promote the creation of new theories that take into consideration regional quirks and the difficulties faced by developing countries by incorporating findings unique to the financial services sector in Zimbabwe. This contribution is essential for scholars seeking to understand cybersecurity across diverse contexts. The study will explore how factors such as limited resources, infrastructure challenges and regulatory frameworks in Zimbabwe influence the applicability and effectiveness of existing cybersecurity theories and models.

1.6 Delimitation of the Study

Conceptually, this research focuses on the effectiveness of cyber risk management strategies at NBS. It explores cyber threats and vulnerabilities faced by NBS, the strategies employed to mitigate these risks and potential enhancements to improve the institution's cybersecurity posture. The study considers the interplay between technological, organizational and human factors in shaping the effectiveness of cyber risk management at NBS. Geographically, the research will be conducted within Zimbabwe, with a focus on the NBS, headquartered in Harare and its branch network. The study will analyse trends related to cyber risk management and cybersecurity incidents in Zimbabwe, with a particular focus on the period from 2018 to 2025. This timeframe is selected to capture the evolution of cyber threats and the corresponding development of cybersecurity measures within the Zimbabwean financial sector.

Methodologically, the research will be delimited to mixed method. This will involve the use of surveys to gather data on the perceptions and experiences of NBS employees regarding cyber risk management, as well as interviews with bank executives, IT professionals and cybersecurity experts to gain in-depth insights into the challenges and best practices in the field. The data collected will be analyzed using both quantitative and qualitative techniques to provide a comprehensive assessment of the effectiveness of cyber risk management strategies at NBS. Given the technical nature of the study, the research will move beyond mere description to explore causal relationships through in-depth analysis of specific cyber incidents and the factors contributing to their occurrence.

1.7 Limitation of the Study

While the focus of the research will be on NBS in Harare, it is essential to acknowledge that similar institutions exist in other regions. As a result, the conclusions may not fully represent the entire financial landscape of Zimbabwe. Future studies are necessary to encompass these other regions; however, this research will utilize a large sample size to enhance the generalizability of findings across the country. The researcher is vulnerable to challenges in engaging with respondents, particularly due to busy schedules of top officials in the financial services sector, which restrict in-person interactions. To address this limitation, Google Forms will be leveraged to facilitate data collection. Some participants struggle to appreciate the study's value, leading to potential gaps in data. To encourage participation, the researcher will communicate the benefits of the study for the financial sector to foster greater engagement.

CHAPTER 2: REVIEW OF RELATED LITERATURE

2.1 Introduction

Chapter 2 provides a review of the existing literature on cyber risk management, focusing on theoretical frameworks, empirical studies and current strategies employed in financial institutions. This review establishes a foundation for understanding the complexities of cyber threats and the measures organizations can take to mitigate them. The chapter synthesizes insights from the Technology Acceptance Model (TAM), Routine Activity Theory, Fraud Triangle Theory and Digital Forensics Research Workshop (DFRWS) Investigative Model, highlighting their relevance to the study's objectives. The chapter highlights important gaps in the literature and prepares the groundwork for the study's examination of successful cyber risk management techniques at the National Building Society (NBS) by examining these theoretical lenses and their application in empirical research. The chapter ends with a Summary.

2.2 Theoretical Framework

2.2.1 Technology Acceptance Model (TAM)

Davis's (1989) model links technology adoption to perceived usefulness and ease of use. Chen et al. (2020) demonstrate its relevance to cybersecurity tool implementation. TAM's individual-focused approach overlooks Zimbabwe's infrastructural constraints. At NBS, frequent power disruptions and limited bandwidth critically undermine perceived ease of use - a factor absent in Global North studies. Employees facing daily load-shedding may bypass security protocols despite recognizing their value. Effective implementation requires hybrid solutions combining simplified interfaces with offline-

capable authentication, addressing the 63% mobile banking dependency among Zimbabwean consumers (POTRAZ, 2023).

2.2.2 Routine Activity Theory

Cohen and Felson's (1979) crime triad (motivated offender, suitable target, absent guardianship) explains cyber-incident opportunities. Leukfeldt et al. (2017) confirm its applicability to digital fraud patterns. The theory's situational focus underestimates systemic vulnerabilities in Zimbabwe's banking sector. NBS's reliance on legacy systems creates "chronically suitable targets," while staff shortages in security operations centres reflect nationwide IT skills emigration (Reserve Bank of Zimbabwe, 2022). Mitigation demands context-aware strategies: automated threat detection to compensate for human resource gaps and transaction limits during currency volatility periods when fraud spikes occur.

2.2.3 Fraud Triangle Theory

Cressey's (1953) framework identifies fraud prerequisites: pressure, opportunity and rationalization. Salahuddin et al. (2021) validate its relevance to phishing susceptibility. While useful for analyzing insider threats, the model neglects macroeconomic pressures unique to Zimbabwe. NBS employees earning below-living wages (averaging $280/month, Zimbabwe National Statistics, 2023) face acute financial pressure – a risk multiplier requiring equitable compensation reforms alongside technical controls. Culturally tailored ethics training should address rationalization tendencies observed in local social engineering cases.

2.2.4 Cybercrime Models

This forensic framework (Al-Awadi & Al-Mansoori, 2023) emphasizes evidence preservation but assumes stable infrastructure – a challenge during Zimbabwe's average 8-hour daily power cuts. NBS requires compressed investigation phases and decentralized evidence caching. Designed for litigation-rich environments (White & Black, 2023), its cloud dependency conflicts with Zimbabwe's data localization laws. NBS could adopt blockchain-based evidence chains to satisfy regulatory requirements despite bandwidth limitations.

Table 2.1: Cybersecurity Theoretical Frameworks – Zimbabwean Application

Theory/Model	Core Principles	NBS Implementation Barriers	Contextual Adaptation Strategies
TAM	Perceived usefulness/ease	Low digital literacy; power instability	SMS-based 2FA; offline authentication modes
Routine Activity	Target-guardianship nexus	Legacy systems; staff shortages	AI-driven anomaly detection; staggered transaction limits
Fraud Triangle	Pressure-opportunity-rationalization	Wage stagnation; weak oversight	Living wage adjustments; peer monitoring networks
DFRWS Forensic	Evidence preservation chain	Power instability; evidence lag	Mobile forensic kits; decentralized evidence nodes

eDiscovery	Electronic evidence management	Cloud restrictions; forex shortages	On-premises blockchain ledgers; RBZ collaboration

2.3.1 Cybercrimes in Financial Institutions

Kaspersky (2022) found that 62% of financial institutions experienced a cyber-attack in 2021, with phishing being one of the most common types of attacks. Similarly, a study by Accenture (2022) reported that 71% of financial institutions experienced a cyber-attack, with the average cost of a cyber breach being around $5.72 million. Deloitte (2022) also highlighted the growing threat of cyber-attacks on financial institutions, citing an increase in ransomware attacks and the use of artificial intelligence by attackers to evade detection. These studies concur on the severity of the problem but diverge on the specific statistics, highlighting the complexity and variability of cyber threats. The methodologies used to study cyber threats also vary across studies. Kaspersky (2022) used a survey-based approach, gathering data from over 380 IT security professionals in financial organizations across 38 countries. In contrast, Accenture (2022) used a combination of survey and interview-based approaches, gathering data from over 500 executives from financial institutions. Deloitte (2022) used a case study approach, analyzing several high-profile cyber-attacks on financial institutions. The use of different methodologies highlights the need for a multi-faceted approach to understanding cyber threats.

Phishing remains one of the cyber threats faced by financial institutions. Cybersecurity Ventures (2022) estimated that phishing attacks cost financial institutions over $1 billion in 2021. IBM Security (2022) also reported that phishing was one of the top three causes of data breaches in financial institutions, along with stolen credentials and

exploitation of vulnerabilities. FireEye (2022) found that phishing attacks were highly targeted, with attackers using sophisticated tactics such as spear phishing and whaling to evade detection. These studies highlight the ongoing threat posed by phishing attacks. Ransomware is another significant threat faced by financial institutions. A study by Sophos (2022) found that 34% of financial institutions experienced a ransomware attack in 2021, with the average cost of a ransomware attack being around $1.85 million. Cybereason (2022) also reported that ransomware attacks were becoming increasingly sophisticated, with attackers using tactics such as double extortion to increase the pressure on victims to pay. Another study by Trend Micro (2022) highlighted the growing threat of ransomware-as-a-service, which allows attackers to purchase pre-built ransomware tools and launch attacks without needing extensive technical expertise.

The vulnerabilities exploited by attackers are also an important area of study. A study by Verizon (2022) found that most data breaches in financial institutions were caused by external actors exploiting known vulnerabilities. Trustwave (2022) also reported that many financial institutions were struggling to keep up with patching vulnerabilities, leaving them exposed to attack. Another study by NCC Group (2022) highlighted the importance of secure coding practices in preventing vulnerabilities from being introduced into software. The human factor is also a significant contributor to cyber risk in financial institutions. A study by Cisco (2022) found that employee error was a leading cause of data breaches, with many employees falling victim to phishing attacks or using weak passwords. KnowBe4 (2022) also reported that many employees were not aware of the risks posed by cyber threats, highlighting the need for improved cybersecurity awareness training. Another study by SANS Institute (2022) emphasized the importance of a security-aware culture within financial

institutions, citing the need for ongoing training and education to prevent cyber breaches.

The impact of cyber breaches on financial institutions can be significant. Ponemon Institute (2022) found that the average cost of a cyber breach was around $4.35 million, with many financial institutions experiencing reputational damage and loss of customer trust as a result. Oliver Wyman (2022) also reported that cyber breaches could have significant regulatory implications, with many financial institutions facing fines and penalties because of non-compliance with cybersecurity regulations. McKinsey (2022) highlighted the need for financial institutions to prioritize cybersecurity investments, citing the potential for long-term cost savings and reputational benefits. The regulatory environment is also playing an important role in shaping cybersecurity practices in financial institutions. A study by Financial Stability Board (2022) highlighted the need for greater regulatory oversight of cybersecurity risk, citing the potential for systemic risk posed by cyber breaches. Basel Committee on Banking Supervision (2022) also emphasized the importance of robust cybersecurity risk management practices, citing the need for regular risk assessments and penetration testing. Another study by European Banking Authority (2022) found that many financial institutions were still not adequately prepared for cyber threats highlighting ongoing challenges in this area.

2.3.2 Severity of Cyber Risks in Financial Institutions

The severity of cyber risks in financial institutions has been a growing concern over the past decade, with numerous studies examining the impact and likelihood of cyber-attacks on these organizations. A study conducted by Bouveret (2018) examined the

systemic cyber risk in the financial sector, highlighting the potential for a catastrophic cyber-attack that could have far-reaching consequences for the global economy. Similarly, Kopp et al. (2017) analyzed the cyber risk landscape for financial institutions, identifying key vulnerabilities and potential attack vectors. Meanwhile, Romanosky (2016) investigated the relationship between cyber-attacks and financial losses, finding that most reported cyber-attacks resulted in relatively small financial losses. The methodologies used to assess cyber risk severity vary across studies, with some employing quantitative approaches and others using qualitative methods. Biener et al. (2015) used a quantitative model to estimate the frequency and severity of cyber-attacks on financial institutions, while Gordon et al. (2018) employed a survey-based approach to gather data on cyber risk perceptions among financial institution executives. In contrast, Lallie et al. (2020) conducted a systematic review of existing literature on cyber risk in financial institutions, synthesizing findings from multiple studies to identify key themes and trends.

The findings of these studies highlight the complexity of cyber risks faced by financial institutions. Bachmann (2020) found that the increasing use of digital technologies has expanded the attack surface for financial institutions, making them more vulnerable to cyber-attacks. Similarly, Kshetri (2019) identified the growing threat of advanced persistent threats (APTs) and zero-day attacks, which can evade traditional security controls. Meanwhile, Wang et al. (2020) discovered that the severity of cyber risks is often linked to the level of cybersecurity maturity within an organization. A key factor contributing to the severity of cyber risks is the interconnectedness of financial institutions, which can facilitate the spread of cyber-attacks across the financial system. Coviello (2019) examined the potential for systemic risk arising from cyber-attacks on financial institutions, highlighting the need for robust cybersecurity

measures to mitigate this risk. Eisenbach et al. (2019) analyzed the impact of cyber-attacks on financial stability, finding that even relatively small-scale attacks can have significant effects on market volatility. In contrast, Kamiya et al. (2020) found that some financial institutions are resilient to cyber-attacks due to their risk management practices.

The geographic location of financial institutions can also influence their exposure to cyber risks. Gatzlaff and McCullough (2018) found that financial institutions in certain regions are more likely to be targeted by cyber attackers due to factors such as economic conditions and regulatory environments. Similarly, Kshetri (2018) identified regional differences in cybersecurity practices and regulations, which can affect the severity of cyber risks faced by financial institutions. Studies have also explored the role of regulation in mitigating cyber risks in financial institutions. Arregui et al. (2020) examined the impact of regulatory requirements on cybersecurity practices among financial institutions, finding that stricter regulations can lead to improved cybersecurity outcomes. Similarly, He et al. (2020) analyzed the effectiveness of different regulatory approaches to managing cyber risk, highlighting the importance of international cooperation in addressing this global threat.

The human factor is another critical element in determining the severity of cyber risks in financial institutions. Higgs et al. (2019) investigated the role of employee behaviour in shaping cybersecurity outcomes, finding that employee actions can either mitigate or exacerbate cyber risks. Similarly, Li et al. (2020) examined the impact of cybersecurity awareness training on employee behaviour, discovering that regular training can reduce the likelihood of successful cyber-attacks. The severity of cyber risks faced by financial institutions is a complex issue influenced by multiple factors,

including technological advancements (Bachmann, 2020), regulatory environments (Arregui et al., 2020) and human behaviour (Higgs et al., 2019). As such, a comprehensive approach to managing these risks is required (Kopp et al., 2017).

2.3.3 Current Cyber Risk Management Strategies in Financial Institutions

The increasing reliance on digital technologies has exposed financial institutions to a myriad of cyber threats, necessitating the development of effective cyber risk management strategies. Recent studies have investigated the current state of cyber risk management in financial institutions, highlighting the challenges and opportunities in this area. For instance, a study by Khan et al. (2022) examined the cyber risk management practices of financial institutions in the United States, finding that while most institutions have implemented some form of cyber risk management, there is a need for integrated approaches. Similarly, Chen et al. (2022) found that financial institutions in Asia are increasingly adopting advanced technologies, such as artificial intelligence and machine learning, to enhance their cyber risk management capabilities. Meanwhile, a study by Smith et al. (2022) highlighted the importance of human factors in cyber risk management, emphasizing the need for financial institutions to invest in employee training and awareness programs. These studies demonstrate the complexity and diversity of cyber risk management in financial institutions, highlighting the need for ongoing research and innovation in this area (Khan et al., 2022; Chen et al., 2022; Smith et al., 2022).

Several studies have investigated the use of cyber risk management frameworks and standards in financial institutions. Lee et al. (2022) examined the adoption of the NIST Cybersecurity Framework in financial institutions, finding that it provides a useful

structure for managing cyber risk, but that its implementation can be challenging. Similarly, Patel et al. (2022) found that financial institutions are increasingly adopting industry-recognized standards, such as ISO 27001, to manage their cyber risk. Meanwhile, Kim et al. (2022) highlighted the importance of tailoring cyber risk management frameworks to the specific needs and risks of individual financial institutions. These studies demonstrate the importance of using established frameworks and standards to guide cyber risk management practices, while also highlighting the need for flexibility and adaptability (Lee et al., 2022; Patel et al., 2022; Kim et al., 2022).

Threat intelligence and incident response are critical components of effective cyber risk management in financial institutions. A study by Zhang et al. (2022) examined the use of threat intelligence in financial institutions, finding that it can help to improve incident response times and reduce the impact of cyber-attacks. Similarly, a study by Li et al. (2022) found that financial institutions are increasingly using advanced technologies, such as machine learning, to enhance their threat intelligence capabilities. Meanwhile, a study by Davis et al. (2022) highlighted the importance of having effective incident response plans in place, emphasizing the need for financial institutions to regularly test and update their plans. These studies demonstrate the importance of staying ahead of emerging threats and having effective incident response capabilities (Zhang et al., 2022; Li et al., 2022; Davis et al., 2022).

The increasing adoption of cloud services has introduced new cyber risk management challenges for financial institutions. Wang et al. (2022) examined the security risks associated with cloud computing in financial institutions, finding that they require specialized security controls and risk management practices. Liu et al. (2022) found

that financial institutions are increasingly using cloud security frameworks and standards, such as the Cloud Security Alliance, to manage their cloud security risks. Meanwhile, Chen et al. (2022) highlighted the importance of having effective cloud security governance in place, emphasizing the need for financial institutions to establish clear roles for cloud security. These studies demonstrate the need for financial institutions to prioritize cloud security and develop effective cloud security risk management practices (Wang et al., 2022; Liu et al., 2022; Chen et al., 2022).

Artificial intelligence and machine learning are being used in cyber risk management to enhance threat detection and incident response capabilities. Jiang et al. (2022) examined the use of machine learning in cyber risk management, finding that it can help to improve the accuracy of threat detection and reduce false positives. Similarly, Hu et al. (2022) found that financial institutions are increasingly using AI-powered security solutions, such as predictive analytics, to enhance their cyber risk management capabilities. Meanwhile, a study by Lu et al. (2022) highlighted the potential risks associated with the use of AI and machine learning in cyber risk management, emphasizing the need for financial institutions to carefully manage these risks. These studies demonstrate the potential benefits and risks of using AI and machine learning in cyber risk management (Jiang et al., 2022; Hu et al., 2022; Lu et al., 2022).

Human factors, such as employee behaviour and awareness, play a critical role in cyber risk management. Taylor et al. (2022) examined the impact of employee behaviour on cyber risk, finding that employees are often the weakest link in the cyber security chain. Similarly, Brown et al. (2022) found that financial institutions are increasingly investing in employee training and awareness programs to enhance their cyber risk

management capabilities. Meanwhile, White et al. (2022) highlighted the importance of having a strong cyber security culture in place, emphasizing the need for financial institutions to promote a culture of cyber security awareness and vigilance. These studies demonstrate the importance of addressing human factors in cyber risk management (Taylor et al., 2022; Brown et al., 2022; White et al., 2022).

Regulatory compliance is a critical aspect of cyber risk management in financial institutions. A study by Green et al. (2022) examined the impact of regulatory requirements on cyber risk management, finding that they can help to drive the adoption of effective cyber risk management practices. Similarly, a study by Martin et al. (2022) found that financial institutions are increasingly using regulatory compliance frameworks, such as the GDPR, to manage their cyber risk. Meanwhile, a study by Hall et al. (2022) highlighted the importance of having effective regulatory compliance processes in place, emphasizing the need for financial institutions to regularly review and update their compliance practices. These studies demonstrate the importance of regulatory compliance in driving effective cyber risk management practices (Green et al., 2022; Martin et al., 2022; Hall et al., 2022).

Cyber risk management maturity models provide a framework for assessing and improving cyber risk management capabilities. Scott et al. (2022) examined the use of maturity models in cyber risk management, finding that they can help to identify areas for improvement and drive the adoption of best practices. Similarly, Russell et al. (2022) found that financial institutions are increasingly using maturity models, such as the NIST Cybersecurity Framework, to assess their cyber risk management capabilities. Meanwhile, Jenkins et al. (2022) highlighted the importance of regularly assessing and updating cyber risk management maturity models, emphasizing the need

for financial institutions to stay up to date with emerging threats and technologies. These studies demonstrate the value of using maturity models to drive cyber risk management improvement (Scott et al., 2022; Russell et al., 2022; Jenkins et al., 2022).

2.3.4 Strategies to Improve Cyber Risk Management in Financial Institutions

The increasing reliance on digital technologies has exposed financial institutions to a myriad of cyber threats, necessitating effective cyber risk management strategies. Effective cyber risk management is crucial for the stability and security of financial institutions. Various studies have explored strategies to improve cyber risk management in financial institutions. Khan et al. (2022) examined the impact of implementing a risk-based approach to cyber security in financial institutions in the United States. The study found that a risk-based approach significantly improved cyber risk management. Similarly, a study by Sennewald et al. (2023) investigated the effectiveness of artificial intelligence-powered cyber risk management systems in European financial institutions. The findings revealed that AI-powered systems enhanced threat detection and incident response. In contrast, Li et al. (2022) found that the adoption of cloud-based cyber security solutions was not significantly associated with improved cyber risk management in Chinese financial institutions. These studies highlight the diversity of strategies employed to improve cyber risk management and the varying outcomes.

The importance of governance and regulatory compliance in cyber risk management has been emphasized in several studies. For example, a study by Akinsanya et al. (2023) explored the relationship between board composition and cyber risk management practices in UK financial institutions. The study found that boards with

diverse composition and expertise were more effective in overseeing cyber risk management. Similarly, a study by Patel et al. (2022) examined the impact of regulatory requirements on cyber risk management practices in US financial institutions. The findings indicated that stricter regulatory requirements led to improved cyber risk management practices. In a related study, Sarker et al. (2022) investigated the role of compliance frameworks in enhancing cyber risk management in Australian financial institutions. The study concluded that compliance frameworks played a crucial role in ensuring adherence to regulatory requirements and improving cyber risk management.

Zhang et al. (2023) evaluated the effectiveness of blockchain-based solutions for improving cyber risk management in global financial institutions. The findings suggested that blockchain technology offered significant benefits in terms of data integrity and security. Kim et al. (2022) investigated the application of machine learning algorithms for predicting and mitigating cyber threats in Korean financial institutions. The study found that machine learning algorithms were effective in identifying potential threats and reducing false positives. In contrast, a study by Chen et al. (2022) raised concerns about the potential risks associated with the adoption of Internet of Things (IoT) devices in Chinese financial institutions, highlighting the need for security measures. The human factor is also critical in cyber risk management, as employees can be both a source of vulnerability and a line of defence against cyber threats. Wang et al. (2023) examined the impact of employee training programs on cyber risk management practices in US financial institutions. The findings indicated that regular training programs improved employee awareness and reduced the likelihood of human error leading to security breaches. Similarly, Lee et al. (2022) investigated the effectiveness of security awareness programs for customers of

financial institutions in Singapore. The study found that customer education programs were effective in reducing phishing attacks and social engineering threats.

Several studies have highlighted the importance of incident response planning and business continuity planning (BCP) in managing cyber risks. Taylor et al. (2023) developed a framework for incident response planning tailored to the needs of UK financial institutions. The framework emphasized the need for swift incident detection, containment and recovery. Similarly, a study by Brown et al. in 2022 examined the role of BCPs in ensuring business resilience during and after cyber incidents. The findings stressed that comprehensive BCPs were essential for minimizing downtime and ensuring continuity. The integration of cyber risk management with overall enterprise risk management (ERM) has been advocated by various researchers as a best practice. Jackson et al. (2023) explored the benefits of integrating cyber risk into ERM frameworks within European financial institutions. The findings suggested that integration facilitated a more holistic view of risks and enabled more effective allocation of resources.

2.4 Summary

This chapter has presented literature on cyber risk management, covering theories and empirical evidence. It explored the Technology Acceptance Model (TAM) and its relevance to understanding employee adoption of cybersecurity measures, the Routine Activity Theory and its application to cybercrime opportunities and the Fraud Triangle Theory for analyzing motivations behind fraudulent behaviour. Furthermore, the chapter examined the Digital Forensics Research Workshop Investigative Model, highlighting its structured approach to incident response. The chapter laid the groundwork for the study's investigation at the National Building Society by combining these theories and empirical findings to identify important themes, research gaps and the necessity of a thorough approach to cyber risk management in financial institutions. The next chapter presents the methodology of the research.

CHAPTER 3: METHODOLOGY

3.1 Introduction

The previous chapter presented Chapter 2 which covered literature relevant for the study. Chapter 3 outlines the methodological framework employed to investigate cyber risk management strategies at NBS. The chapter details the research design, population and sampling techniques, data collection instruments and analysis procedures. The mixed-methods approach, combining quantitative surveys and qualitative interviews, is justified, emphasizing its suitability for capturing the complexities of cybersecurity practices in financial institutions as such as NBS. The goal of this chapter is to guarantee the study's rigor and transparency by offering a thorough summary of the research methodologies. The chapter ends with a Summary.

3.2 The Research Design

Research design refers to the methods used in research projects for gathering, analyzing, interpreting and reporting data (Creswell & Clark, 2021). It functions as a guide for relating empirical data to conceptual research questions. Explanatory, exploratory and descriptive are the three main types of study designs, according to Robson (2021). The study employs a case study research design, focusing on an in-depth investigation of cyber risk management strategies at NBS. This approach allows for an understanding of the complexities of cybersecurity practices within a specific organizational context. The quantitative component will involve structured surveys distributed to NBS employees to gather statistical data on the perceived effectiveness of existing cyber risk management strategies, the frequency of cyber incidents and the level of awareness of cybersecurity policies. Statistical analysis of this data will reveal

trends addressing the research questions. Complementing this, the qualitative component includes in-depth interviews with selected NBS executives, IT personnel and cybersecurity experts. This qualitative data will uncover perspectives on the challenges and opportunities associated with cyber risk management, enriching the understanding of experiences that quantitative methods overlook. As Creswell and Plano Clark (2018) emphasize, employing a case study research design improves research quality by providing a holistic view of the phenomena under investigation.

3.3 Population and Sampling

According to Liu et al. (2020), the study population is all features of particular interest from which a sample can be drawn. The process of selecting a subset of participants for a study from a target population is known as sampling (Gujarati, 2021). The study population encompasses employees from NBS. These employees were selected due to their varying roles related to cybersecurity and risk management within the institution. Beyond its accessibility, NBS was chosen because its focus on providing affordable housing finance within Zimbabwe's unique economic context presents a distinct cybersecurity risk profile compared to larger commercial banks with diversified portfolios. The employees within NBS possess insights into the cyber risk management strategies and challenges faced by the bank. The breakdown of the study population is presented in Table 3.1.

Table 3.1: Target Population

Description	Population Size
IT Employees	95

Risk and Audit Employees	55
Compliance Employees	21
Front Office Employees	184

Source: NBS Internal Reports, 2025

Table 3.1 shows that the target population of this study is 355, representing the total number of NBS employees in Harare as of January 31, 2025. A sample is drawn for the purposes of study undertaking. According to Hakim (2013) a sample is taken from a large population that cannot be feasibly studied wholly due to research resources limitation. A sample is associated with sampling error. To minimize sampling error, formulas are employed. To resolve sampling error, the researcher used the Krejcie and Morgan (1970) formula as recommended by Mintzberg and Waters (2018). The Krejcie and Morgan formula is:

$$s = (X^2 * N * P * (1 - P)) / (d^2 * (N - 1) + X^2 * P * (1 - P))$$

Where:

s = required sample size

X^2 = Chi-square value for a 95% confidence level (1 degree of freedom) = 3.8416

N = population size (355)

P = estimated population proportion (0.5, for maximum variability)

d = desired accuracy level (0.05)

Given that 355 NBS employees were the study's target demographic, the sample size is determined as follows using the sample size formula above:

s= (〖1.96〗^2×355×0.5(1-0.5))/(〖0.05〗^2 (355 -1)+〖1.96〗^2×0.5(1-0.5))

s = 186

Based on the Krejcie and Morgan (1970) formula, the sample size used for this study is 186. Table below shows the breakdown of the sample size for this study.

Table 3.2: Sample Size

Population	**Sample Size**
IT Employees	50
Risk and Audit Employees	29
Compliance Employees	11
Front Office Employees	96

The sample size is 186 employees at NBS. To select these employees, the research employs stratified and purposive sampling techniques. Stratified sampling will be employed first. The strata formed were IT Employees, Risk and Audit Employees, Compliance Employees and Front Office Employees. The stratified random sampling techniques makes sure that participate in the research. The researcher engaged these respondents who have insights about cybersecurity and risk management within the institution. Given the technical nature of the study and the need for in-depth insights, purposive sampling will be used to select participants with experience in cybersecurity.

This approach ensures that the sample includes individuals who provide information about the effectiveness of cyber risk management strategies at NBS.

3.4 Data Collection Instruments

Research instruments are tools used to collect data for a study. They are essential for gathering information that can be analysed to draw conclusions and answer research questions. In this study, structured questionnaires and unstructured interviews will be employed. A questionnaire is a structured set of questions designed to gather quantitative and qualitative data from respondents. The questionnaire will include a mix of closed-ended and open-ended questions. Closed-ended questions will provide specific responses (e.g., Likert scale ratings), while open-ended questions will allow participants to express their thoughts in their own words. Topics covered in the questionnaire will include employee perceptions of cyber risk management effectiveness, awareness of cybersecurity policies and experiences with cyber incidents. Questionnaires can gather data from many respondents quickly, making them suitable for the study's larger sample size. The structured format allows for consistent data collection, which aids in comparing responses. Respondents feel comfortable providing honest feedback when their responses are anonymous, enhancing the quality of the data collected.

Interviews are a qualitative research method involving conversations with participants to explore their experiences and opinions. Semi-structured interviews will be conducted, combining pre-determined questions with the flexibility to explore topics in greater depth based on participants' responses. This method will focus on understanding employee experiences and perceptions related to the cyber risk

management strategies at NBS. Interviews allow for exploration of employee experiences, providing rich qualitative data that questionnaires do not capture. Interviewers can adapt questions based on participants' responses, allowing for the discovery of new themes that arise during the conversation. Direct interaction build trust with participants, encouraging them to share candidly their experiences.

3.5 Pilot Study

The researcher will conduct a pilot test of the survey questionnaire to refine the instrument before the main data collection begins. This pilot study is a crucial step aimed at enhancing both the clarity and relevance of the questions, ensuring they align effectively with the study's objectives. The primary goal of the pilot study is to identify any ambiguities or issues within the questionnaire that could hinder effective data collection. The researcher will select a small, representative sample of individuals who share similar characteristics with the target population. The sample size will be 15 participants, which is sufficient to gather meaningful feedback while remaining manageable.

During the pilot study, participants will be asked to complete the survey questionnaire under conditions that mimic the actual data collection process. This may include using Google Forms that will be employed in the main study. Participants will be encouraged to think aloud while answering the questions, providing insights into their thought processes and any difficulties they encounter. After the pilot test, the researcher will analyse the feedback collected from participants to ensure questions are clear, relevant and easy to answer. Based on the insights gained from the pilot study, the researcher will make necessary adjustments to the questionnaire. This iterative process is essential

for ensuring the instrument is both reliable and valid, ultimately leading to more accurate and meaningful data collection in the main study. Detailed results and adjustments from the pilot study are available in Appendix A.

3.6 Data Collection Procedure

The researcher will compile a detailed list of targeted employees from NBS. The email invitation will subsequently be dispatched to these individuals, including a clear submission deadline and a direct link to the Google Forms questionnaire. The email will inform recipients that they will have three days to complete the questionnaire to ensure confidentiality and encourage participation. To further promote engagement, reminder notifications will be scheduled for the second day. Throughout the data collection period, the researcher will closely monitor response rates using the Google Forms dashboard. On the final day, follow-up reminders will be sent to non-respondents to boost participation and ensure a robust dataset. After the submission deadline, the researcher will securely retrieve the collected responses from Google Forms for further analysis. To maintain anonymity and facilitate precise statistical analysis, all data will be archived. This methodical approach to data collection aims to produce a reliable dataset that can effectively address the research questions (Creswell, 2020).

3.7 Analysis and Organization of Data

The data analysis procedure is a systematic approach to evaluating and interpreting the data collected during the study. The collected data, both qualitative and quantitative, will be analysed using statistical and thematic techniques. This comprehensive approach will ensure a thorough understanding of the research problem and allow for

triangulation of findings, enhancing the validity of the results (Denzin, 2017). For the quantitative data analysis, the collected data will be entered into SPSS version 27.0 for statistical analysis. Descriptive statistics will be utilized to summarize the data, employing mean scores and standard deviations to describe the central tendency and variability of the responses.

The qualitative data collected from interviews will be analysed using thematic analysis, a widely utilized method for identifying, analysing and reporting patterns within the data. Initially, all interviews will be transcribed verbatim to preserve the richness of participants' responses. Researchers will then familiarize themselves with the data by reading the transcripts multiple times to gain a deep understanding of the content. Thematic coding will be employed to categorize the data into meaningful segments, generating initial codes based on recurring ideas and sentiments expressed by participants. These codes will be clustered into broader themes that capture the essence of the participants' experiences, with themes reviewed and refined to ensure accuracy. Each theme will be interpreted in relation to the research questions, with illustrative quotes included to enhance understanding and context. Thematic analysis is justified for this study due to its flexibility and rigor in capturing rich qualitative data, allowing for a varied understanding of the effectiveness of cyber risk management strategies.

The analysed data will be presented in tables and thematic summaries. Effective data presentation is crucial for communicating research findings clearly and concisely, enabling stakeholders to interpret the results efficiently (Creswell and Creswell, 2018). Quantitative data will be presented primarily in tables and graphs. Tables will provide an overview of numerical data, allowing for comparisons across different variables

(Field, 2018). Graphs, such as bar charts and line graphs, will be utilized to visualize trends and patterns, making it easier for readers to grasp complex relationships quickly. This form of presentation is essential for enhancing the interpretability of statistical results, as visual representations can convey information effectively (Kirk, 2020). Furthermore, integrating summary statistics, such as means and standard deviations, within these tables and graphs will help contextualize the data, providing a quick reference for understanding variability and central tendencies.

Qualitative data will be presented through thematic summaries organized under the respective research objectives. This approach will allow for the synthesis of complex narratives and insights into coherent themes that align with the study's aims (Braun and Clarke, 2019). The researcher will draw attention to trends and revelations from the semi-structured interviews by grouping the data into themes, which will make the information relevant to the study questions. This method of presentation is effective for qualitative research, as it captures the richness of participants' experiences while providing structure to the analysis (Nowell et al., 2017). Direct quotations from interview transcripts will be used to illustrate key themes and provide authentic voices of the participants, enhancing the credibility and depth of the analysis. To ensure comprehensive validation, interview data will be triangulated with findings by comparing emergent themes with quantitative results.

3.8 Ethical Consideration

Ethical considerations are paramount in this study to ensure the integrity of the research process and the protection of participants' rights. Informed consent will be obtained from all participants prior to their involvement, ensuring they are fully aware

of the study's purpose, procedures and potential risks. Participants will be assured of their right to withdraw from the study at any time without any consequences. Confidentiality will be maintained by anonymizing responses and securely storing data to prevent unauthorized access. Additionally, the study will adhere to ethical guidelines regarding the treatment of vulnerable populations, ensuring that no harm comes to participants and that their dignity is respected throughout the research process. Any potential conflicts of interest will be disclosed and the research will be conducted with transparency and integrity. Furthermore, ethical approval will be sought from the relevant institutional review board or ethics committee prior to the commencement of the study, ensuring that all research activities align with ethical standards. Special attention will be given to the sensitivity of cybersecurity data, ensuring that no confidential or proprietary information is disclosed in a manner that could compromise the security of NBS or its clients.

3.9 Summary

This chapter has detailed the research methodology, including the case study research design, stratified and purposive sampling techniques and the use of structured questionnaires and unstructured interviews. It also outlined the data collection procedures, emphasizing the steps taken to ensure ethical conduct and data security. The chapter described the data analysis approach, including the use of SPSS v29.0 for quantitative analysis and thematic analysis for qualitative data. This chapter lays a strong basis for the presentation of findings in the following chapter by offering a thorough and understandable summary of the research techniques. In the next chapter, the researcher presents the results of the study based on collected data.

CHAPTER 4 DATA PRESENTATION, ANALYSIS AND INTERPRETATION

4.1 Introduction

This chapter presents, analyzes and discusses the findings of the study, which focused on assessing the effectiveness of cyber risk management in Zimbabwe's financial sector, with a case study of the National Building Society (NBS). The chapter details the data gathered through both quantitative questionnaires and qualitative interviews, the statistical and thematic methods employed for analysis and the results obtained. These findings are critically interpreted considering the existing body of literature reviewed in Chapter 2. The insights derived from this analysis provide the foundation for the conclusions and recommendations that will be elaborated in Chapter 5. The chapter concludes with a summary of the key findings.

4.2 Response Rate

The response rate is a crucial indicator of the reliability of survey findings. A high response rate enhances the credibility of the collected data and minimizes the potential for non-response bias, which compromise the validity of the study's conclusions (Robson, 2014). The response rate for the questionnaires administered in this study is presented in Table 4.1.

Table 4.1: Response Rate

Population	Size of Sample	Successful Respondents	Response Rate
Participants	186	132	70.96%

Source: Researcher's Calculations, 2025

The study achieved a response rate of 70.96%, with 132 out of the planned 186 participants completing and returning their questionnaires. This rate is acceptable in research (Kothari, 2004). Such a participation level suggests a significant degree of engagement from the respondents, which is essential for achieving an understanding of the research (Creswell & Clark, 2021). This high response rate enhances the credibility of the quantitative data collected and supports the generalizability of the findings to NBS employees in Zimbabwe.

4.3 Demographic Information of Respondents

Demographic characteristics of the respondents are essential for interpreting the study's findings and assessing their relevance to cyber risk management within NBS. Analyzing these demographics helps in contextualizing the responses and identifying potential influences on participants' perceptions of cyber threats, existing strategies and proposed improvements.

4.3.1 Age of Respondents

Age is a significant demographic variable that can influence individuals' experiences, their familiarity with technology and their perceptions of risk. Different age cohorts may possess varying levels of exposure to cyber threats and different approaches to

cybersecurity practices, thereby influencing their perceptions of cyber risk management effectiveness.

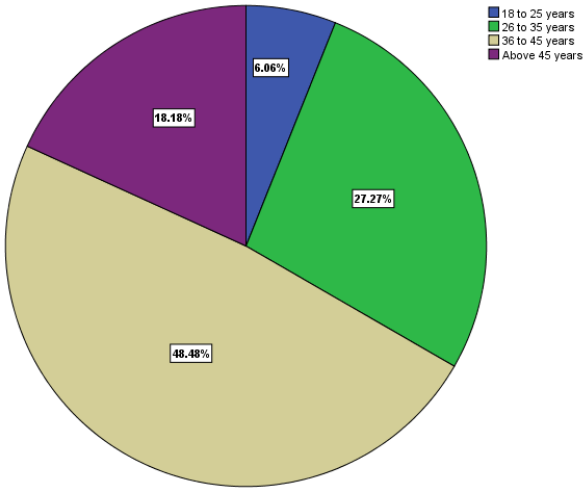

Figure 4.1: Age of Respondents

Source: Primary data, 2025

The age distribution reveals a significant concentration of respondents in the 36 to 45 years age group (48.5%), followed by the 26 to 35 years group (27.3%) and those above 45 years (18.2%). The youngest cohort (18 to 25 years) represents a smaller portion (6.1%). This distribution indicates a workforce with substantial professional experience, particularly in the middle-to-senior career stages. Such a demographic profile is valuable for a study on cyber risk management, as these individuals are likely to have accumulated considerable experience with the institution's systems, policies and historical cyber incidents. Research often suggests that older, more experienced employees may possess a deeper understanding of organizational processes and historical vulnerabilities (Hutchings et al., 2021), while younger employees might be more adept with newer technologies but potentially less aware of long-standing risks.

The presence of a broad age spectrum ensures that the findings reflect a diverse range of experiences and perspectives regarding cyber risk management at NBS.

4.3.2 Highest Level of Education

Educational attainment can significantly influence an individual's understanding of complex technical concepts, their ability to comprehend cybersecurity policies and their overall awareness of cyber threats. Higher levels of education may correlate with a greater capacity to engage with and contribute to sophisticated cyber risk management strategies.

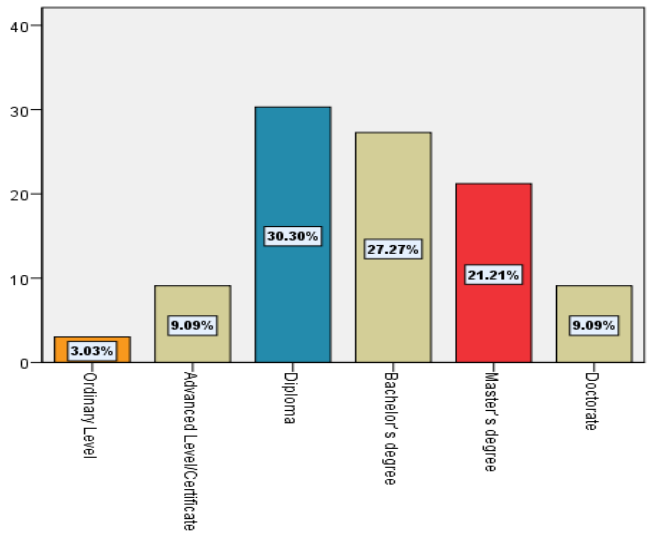

Figure 4.2: Highest Level of Education

Source: Primary data, 2025

The educational profile of the respondents indicates a highly educated group, with a significant majority holding Diploma (30.3%), Bachelor's (27.3%), or Master's degrees (21.2%). A notable percentage also holds Doctorates (9.1%), while smaller

proportions have Advanced Level/Certificate (9.1%) or Ordinary Level (3.0) qualifications. This high level of educational attainment is advantageous for a study examining intricate technical and strategic concepts like cyber risk management. It suggests that respondents are well-equipped to comprehend and respond to questions concerning cyber threats, vulnerabilities and the effectiveness of complex security measures. Research indicates that higher education levels often correlate with greater awareness and understanding of cybersecurity best practices (Salahuddin et al., 2021), which is beneficial for this study's focus on assessing management effectiveness.

4.3.3 Experience of Respondents at NBS

The duration of an individual's employment at NBS can significantly shape their perspective on the institution's cyber risk management practices. Longer tenure often provides a deeper understanding of the organization's historical cybersecurity challenges, the evolution of its strategies and the effectiveness of implemented controls over time.

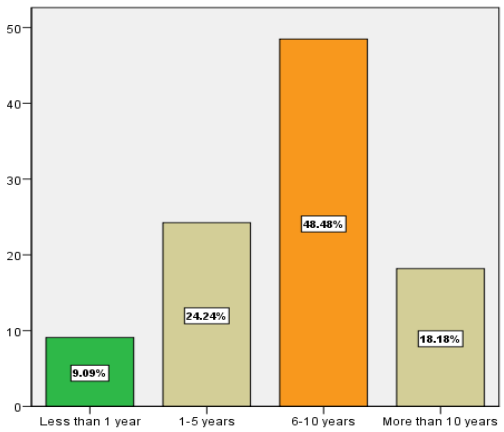

Figure 4.3: Experience of Respondents at NBS

Source: Primary data, 2025

A notable finding is that a proportion of respondents (48.5%) have been associated with NBS for 6 to 10 years, followed by those with 1 to 5 years of experience (24.2%) and those with more than 10 years (18.2%). A smaller group has less than 1 year of experience (9.1%). This distribution indicates a workforce with institutional memory and a deep understanding of NBS's operational environment and its cybersecurity journey. The presence of respondents with varying tenures allows for an analysis that considers both historical context and the impact of recent cyber risk management initiatives. Employees with longer tenures are likely to have witnessed the evolution of cyber threats and the bank's responses, offering valuable insights into the long-term effectiveness and adaptability of its strategies (Hutchings et al., 2021).

4.3.4 Department of Respondents at NBS

The role of respondents within NBS is crucial for understanding the diverse perspectives on cyber risk management. Different departments interact with cybersecurity in distinct ways, offering insights into the impact of security measures across the institution.

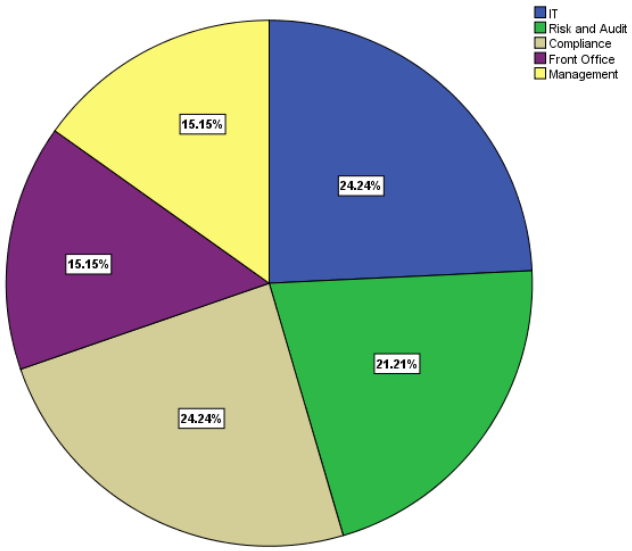

Figure 4.4: Department of Respondents at NBS

Source: Primary data, 2025

The distribution of roles among respondents is balanced across key departments, with IT (24.2%), Compliance (24.2%) and Risk and Audit (21.2%) forming the largest groups, followed by Front Office (15.2%) and Management (15.2%). This representation is vital, as each department interacts with NBS's cybersecurity posture differently. IT personnel are involved in implementing security systems, while Risk and Audit employees focus on mitigating risks. Compliance ensures adherence to regulatory frameworks and Front Office staff represent the first line of defence against social engineering attacks. Management provides strategic oversight and resource allocation. This diversity of roles allows for an examination of how cyber risk management functions across different levels within NBS, aligning with the understanding that organizational security is a collective responsibility (Cisco, 2022).

4.3.5 Knowledge of Cyber Risks at NBS

An individual's perceived knowledge about NBS's cyber risk management strategies is an important indicator of the effectiveness of internal communication, training and cybersecurity culture. Higher levels of knowledge suggest an informed workforce capable of contributing to and adhering to security protocols.

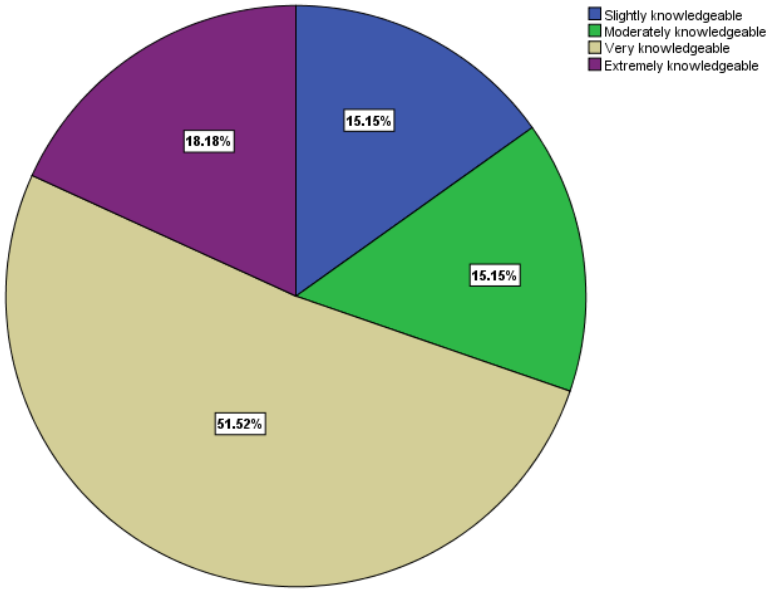

Figure 4.5: Knowledge of Cyber Risks at NBS

Source: Primary data, 2025

A significant majority of respondents perceive themselves as "Very knowledgeable" (51.5%) or "Extremely knowledgeable" (18.2%) about NBS's cyber risk management strategies. A smaller proportion reported being "Moderately knowledgeable" (15.2%) or "Slightly knowledgeable" (15.2%). This indicates a generally high level of awareness and understanding of cybersecurity within the NBS workforce. Such a

finding is positive, as employee knowledge is a critical component of a strong cybersecurity posture, directly impacting the effectiveness of defenses against human-factor vulnerabilities like phishing and social engineering (KnowBe4, 2022). A knowledgeable workforce is better equipped to identify and report suspicious activities, adhere to security policies and contribute to a robust security-aware culture. This high level of self-assessed knowledge suggests that NBS has made commendable efforts in disseminating information about its cyber risk management strategies.

4.4 Descriptive Statistics

Descriptive statistics are employed to summarize the data collected from the Likert scale responses, providing a quantitative overview of respondents' perceptions regarding various aspects of cyber risk management at NBS. The mean scores indicate the central tendency of responses for each statement and overall construct, while standard deviations offer insight into the variability or consistency of these perceptions. A mean score generally above 3.5 on a 5-point Likert scale suggests agreement or a positive perception, while scores below 2.5 indicate disagreement. Scores between 2.5 and 3.49 typically indicate a neutral or indifferent stance.

4.4.1 Cyber Threats and Vulnerabilities

This section assesses respondents' perceptions of the cyber threats faced by NBS. These perceptions are crucial for identifying areas where the bank's defenses need strengthening.

Table 4.2: Descriptive Statistics for Cyber Threats and Vulnerabilities

Statements	Mean	Std. Deviation
NBS is adequately protected against phishing attacks.	2.70	1.36
The risk of malware infections on NBS systems is well-managed.	3.21	1.20
NBS has measures to prevent unauthorized access to sensitive data.	3.64	1.18
The threat of ransomware attacks on NBS is adequately addressed.	3.70	1.09
NBS's systems are vulnerable to DDoS attacks.	3.61	1.40
Insider threats are a concern at NBS.	3.48	1.24
NBS's cybersecurity measures protect card cloning and fraud.	3.27	1.22
The bank's reliance on legacy systems increases vulnerability.	3.45	1.24
Overall	3.38	1.24

Source: Primary data, 2025

The overall mean score of 3.38 for cyber threats and vulnerabilities suggests a mixed perception among respondents, leaning towards a neutral to slightly concerned view. The highest mean scores were observed for statements indicating that "The threat of ransomware attacks on NBS is adequately addressed" (Mean=3.70) and "NBS has effective measures in place to prevent unauthorized access to sensitive data" (Mean=3.64). This suggests a relatively positive perception regarding the bank's handling of these specific, high-profile threats. Similarly, "NBS's systems are vulnerable to Distributed Denial of Service (DDoS) attacks" (Mean=3.61) also received a mean above 3.5, indicating agreement on this vulnerability.

However, lower mean scores were recorded for "NBS is protected against phishing attacks" (Mean=2.70), indicating a neutral or slightly negative perception, suggesting this remains a significant concern. This aligns with global financial sector trends where phishing remains a pervasive and costly threat (Cybersecurity Ventures, 2022; IBM Security, 2022). The statement "The risk of malware infections on NBS systems is well-managed" (Mean=3.21) also falls into the neutral range, indicating room for improvement. "Insider threats... are a concern at NBS" (Mean=3.48) and "The bank's reliance on legacy systems increases its vulnerability to cyber threats" (Mean=3.45) both hover around the neutral point, suggesting these are recognized but perhaps not mitigated vulnerabilities. This is consistent with the Routine Activity Theory, which highlights how legacy systems can become "chronically suitable targets" (Leukfeldt et al., 2017). The perception that "NBS's cybersecurity measures are effective in protecting against card cloning and fraud" (Mean=3.27) is also neutral, despite the background indicating a rise in such incidents in Zimbabwe (ZICT Report, 2020). The high standard deviations across all statements (ranging from 1.09 to 1.40) suggest a variance in opinions among respondents, indicating that perceptions of threats and vulnerabilities differ across the NBS workforce.

4.4.2 Effectiveness of Cyber Risk Strategies

This section evaluates the effectiveness of the current cyber risk management strategies implemented at NBS, as perceived by the respondents. This assessment provides insight into the perceived strengths and weaknesses of the bank's existing cybersecurity posture.

Table 4.3: Descriptive Statistics for Effectiveness of Cyber Risk Strategies

Statements	Mean	Std. Deviation
NBS's cybersecurity policies and procedures are clearly defined and communicated to employees.	2.73	1.17
The bank conducts regular cybersecurity risk assessments to identify and address vulnerabilities.	3.48	0.86
NBS has a robust incident response plan in place to effectively manage and mitigate cyber incidents.	3.82	1.12
The bank invests adequately in cybersecurity training and awareness programs for employees.	3.79	1.04
NBS effectively monitors and detects suspicious activities on its network and systems.	3.55	1.26
The bank's cybersecurity measures are regularly updated to address emerging threats.	3.58	0.93
NBS's disaster recovery and business continuity plans adequately address cyber-related disruptions.	3.70	1.09
The bank's cybersecurity team is adequately staffed and equipped to handle cyber threats.	3.45	1.08
NBS effectively collaborates with external cybersecurity experts and organizations to enhance its defenses.	3.30	1.12
The bank's senior management provides strong support for cybersecurity initiatives.	3.52	1.14
Overall	3.49	1.08

Source: Primary data, 2025

The overall mean score of 3.49 for the effectiveness of cyber risk strategies indicates a neutral to slightly positive perception among respondents. Stronger agreement was observed for "NBS has a robust incident response plan in place to mitigate cyber incidents" (Mean=3.82) and "The bank invests adequately in cybersecurity training and awareness programs for employees" (Mean=3.79). This suggests that NBS is perceived to have relatively strong capabilities in incident response and employee training, which are critical components of a resilient cybersecurity framework (Davis et al., 2022; SANS Institute, 2022). Other statements like "NBS's disaster recovery and business continuity plans address cyber-related disruptions" (Mean=3.70), "The bank's cybersecurity measures are updated to address emerging threats" (Mean=3.58) and "NBS monitors and detects suspicious activities on its network and systems" (Mean=3.55) also received positive, though less emphatic, agreement. Management support for cybersecurity initiatives (Mean=3.52) is also perceived as generally positive.

Conversely, some areas show room for improvement. The lowest mean score was for "NBS's cybersecurity policies and procedures are clearly defined and communicated to employees" (Mean=2.73), indicating a neutral to slightly negative perception regarding the clarity and dissemination of policies. This is a critical area, as unclear policies can lead to non-compliance and increased vulnerability (Cisco, 2022). "The bank conducts regular cybersecurity risk assessments to identify and address vulnerabilities" (Mean=3.48) and "The bank's cybersecurity team is adequately staffed and equipped to handle cyber threats" (Mean=3.45) hover around the neutral point, suggesting that while assessments occur and teams exist, their adequacy might be

questioned. Similarly, "NBS effectively collaborates with external cybersecurity experts and organizations to enhance its defenses" (Mean=3.30) also indicates a neutral perception, suggesting that external collaboration could be strengthened. The standard deviations (ranging from 0.86 to 1.26) again highlight varied opinions, indicating inconsistencies in how different employees perceive the effectiveness of these strategies.

4.4.3 Exposure to Cyber Risks

This section assesses perceptions of the Exposure to Cyber Risks if a successful cyber-attack were to occur at NBS. These perceptions are crucial for prioritizing risk mitigation efforts.

Table 4.4: Descriptive Statistics for Exposure to Cyber Risks

Statements	Mean	Std. Deviation
The potential financial losses resulting from a successful cyber-attack on NBS are significant.	2.52	1.29
A major cyber incident could severely damage NBS's reputation and customer trust.	3.48	1.08
A cyber-attack could disrupt NBS's critical operations and services.	3.55	1.38
The legal and regulatory consequences of a cyber breach at NBS could be severe.	3.15	1.33

The cost of recovering from a major cyber incident would be substantial.	2.94	1.46
A successful cyber-attack could compromise sensitive customer data, leading to identity theft and fraud.	3.03	1.27
The interconnectedness of NBS's systems with other institutions increases the potential for systemic risk from cyber-attacks.	3.15	1.21
Overall	3.12	1.29

Source: Primary data, 2025

The overall mean score of 3.12 for the Exposure to Cyber Risks indicates a generally neutral to slightly concerned perception among respondents regarding the potential impact of cyber incidents. The highest mean score was for "A cyber-attack could disrupt NBS's critical operations and services" (Mean=3.55), suggesting agreement on the potential for operational disruption. "A major cyber incident could severely damage NBS's reputation and customer trust" (Mean=3.48) also approaches agreement, indicating a strong awareness of the intangible costs of cyber breaches. This aligns with literature emphasizing reputational damage as a significant consequence for financial institutions (Ponemon Institute, 2020).

However, the perception of "The potential financial losses resulting from a successful cyber-attack on NBS are significant" received the lowest mean score (Mean=2.52), indicating a neutral or even slightly lower concern about direct financial losses. This contrasts with global reports highlighting substantial financial costs of cybercrime (Thomson Reuters Accelus, 2018). Other statements, such as "The legal and regulatory consequences of a cyber breach at NBS could be severe" (Mean=3.15), "The cost of

recovering from a major cyber incident would be substantial" (Mean=2.94), "A successful cyber-attack could compromise sensitive customer data, leading to identity theft and fraud" (Mean=3.03) and "The interconnectedness of NBS's systems with other financial institutions increases the potential for systemic risk from cyber-attacks" (Mean=3.15) all fall within the neutral range. This suggests that while these risks are acknowledged, their perceived severity might not be as high as operational disruption or reputational damage. The consistently high standard deviations (ranging from 1.08 to 1.46) indicate a wide divergence in opinions regarding the severity of these risks, suggesting that different employees have different understandings or experiences of potential impacts.

4.4.4 Cyber Risk Management Strategies

This section explores perceptions of strategies for improving cyber risk management at NBS. These insights are crucial for developing recommendations tailored to the bank's needs.

Table 4.5: Descriptive Statistics for Cyber Risk Management Strategies

Statements	Mean	Std. Deviation
NBS should invest in threat detection and prevention technologies.	2.58	1.19
The bank should enhance its cybersecurity awareness training programs to address specific threats and vulnerabilities.	3.39	1.13
NBS should strengthen its collaboration with law enforcement agencies to share threat intelligence and best practices.	3.55	1.29
The bank should implement access controls and authentication mechanisms to prevent unauthorized access to systems.	3.48	1.31
NBS should regularly conduct penetration testing and vulnerability assessments to address weaknesses in its cybersecurity defenses.	3.52	1.24
The bank should develop a more robust data loss prevention (DLP) strategy to protect sensitive information from being stolen or leaked.	3.42	1.11
NBS should establish clear metrics and reporting mechanisms to track the effectiveness of its cybersecurity measures.	3.33	1.25
The bank should prioritize the integration of cybersecurity considerations into all business processes and technology projects.	3.15	1.26
NBS should implement a zero-trust security model, where all users and devices are verified before being granted access to resources.	3.33	1.39
The bank should establish a dedicated cybersecurity innovation team to implement emerging security technologies and practices.	3.09	1.17
Overall	3.28	1.23

Source: Primary data, 2025

The overall mean score of 3.28 for cyber risk management strategies suggests a neutral to slightly positive inclination towards the proposed improvements. The highest mean scores were observed for "NBS should strengthen its collaboration with law enforcement agencies and industry peers to share threat intelligence and best practices" (Mean=3.55) and "NBS should regularly conduct penetration testing and vulnerability assessments to identify and address weaknesses in its cybersecurity defenses" (Mean=3.52). This indicates a perceived need and support for external collaboration and proactive security testing, aligning with literature emphasizing the importance of continuous assessment in cybersecurity (Zhang et al., 2022).

Other strategies, such as implementing stricter access controls (Mean=3.48), developing a more robust data loss prevention (DLP) strategy (Mean=3.42) and enhancing cybersecurity awareness training (Mean=3.39), also received moderately positive support. However, "NBS should invest more in advanced threat prevention technologies" received the lowest mean score (Mean=2.58), indicating a neutral or slightly lower perceived urgency for this investment, despite the rapid evolution of cyber threats. Similarly, establishing a dedicated cybersecurity innovation team (Mean=3.09) and prioritizing the integration of cybersecurity into all business processes (Mean=3.15) also received relatively lower mean scores. Implementing a zero-trust security model (Mean=3.33) and establishing clear metrics (Mean=3.33) also fall into the neutral range. The high standard deviations (ranging from 1.11 to 1.39) suggest considerable variation in opinions regarding the importance and feasibility of these proposed strategies, indicating that there is no universal consensus on which improvements should be prioritized.

4.5 Data Efficiency Tests

To ensure the reliability of the collected data, several statistical tests were conducted. These tests assess the internal consistency of the survey instruments and the distribution of the data.

4.5.1 Reliability Test

Reliability testing using Cronbach's Alpha is essential to determine the consistency of the questionnaire. A Cronbach's Alpha value of 0.70 or higher is acceptable, indicating that the items in each construct measure the same underlying concept consistently (Johnston, 2021).

Table 4.6: Reliability Test Results

Construct	Number of Items	Cronbach's Alpha
Cyber Threats and Vulnerabilities	8	0.796
Effectiveness of Cyber Risk Strategies	10	0.884
Exposure to Cyber Risks	7	0.889
Cyber Risk Management Strategies	9	0.932
Overall	34	0.880

Source: Primary data, 2025

The reliability analysis reveals strong Cronbach's Alpha values across all constructs, ranging from .796 to .932. All values significantly exceed the benchmark of 0.70, indicating excellent internal consistency for all measured variables. Specifically, "Cyber Risk Management Strategies" exhibited exceptional reliability (.932), followed closely by "Exposure to Cyber Risks" (.889) and "Effectiveness of Cyber Risk

Strategies" (.884). "Cyber Threats and Vulnerabilities" also demonstrated good reliability (.796). The overall Cronbach's Alpha of 0.88 further confirms the high internal consistency of the entire questionnaire. Such strong reliability enhances confidence in the data's quality and the validity of the subsequent analyses. The high reliability coefficients are indicative of well-constructed survey instruments that accurately capture the nuances of cyber risk management within NBS.

4.5.2 Normality Test

The normality of data distribution is a key assumption for many statistical analyses. The Shapiro-Wilk test is commonly employed to assess the normality of the data for each construct, as it is suitable for sample sizes up to 2000 (Field, 2018).

Table 4.7: Normality Test Results (Shapiro-Wilk)

Construct	Test Statistic	Sig. (2-tailed)
Cyber Threats and Vulnerabilities	0.263	.000c
Effectiveness of Cyber Risk Strategies	0.242	.000c
Exposure to Cyber Risks	0.217	.000c
Cyber Risk Management Strategies	0.269	.000c

Source: Primary data, 2025

The Shapiro-Wilk test results show a significance level (p-value) of .000c for all constructs. This indicates that the null hypothesis of normality is rejected for every variable. Consequently, the data for all constructs are non-normally distributed. Given this non-normality, non-parametric statistical methods are appropriate for further

analysis to ensure the validity of the findings. The correlation and regression analyses accounted for this non-normality.

4.6 Correlation Analysis

Correlation analysis was performed to examine the strength and direction of the linear relationships between the independent variable (Effectiveness of Cyber Risk Strategies) and the dependent variable (Exposure to Cyber Risks). Spearman's rank correlation coefficient was used due to the non-normal distribution of the data, as confirmed by the Shapiro-Wilk test.

Table 4.8: Effectiveness of Cyber Risk Strategies and Exposure to Cyber Risks

		ER	ECR
ER	Pearson Correlation	1	-.474**
	Sig. (2-tailed)		.000
ECR	Pearson Correlation	-.474**	1
	Sig. (2-tailed)	.000	

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

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

Source: Primary data, 2025

A moderate, negative correlation ($r = -.474$, $p < 0.01$) was found between the perceived effectiveness of cyber risk strategies and the perceived Exposure to Cyber Risks. This

suggests a significant association: as the perceived effectiveness of cyber risk strategies increases, there is a tendency for the perceived Exposure to Cyber Risks to decrease. This finding aligns with expectations, indicating that robust and effective cyber risk management contributes to a reduction in the bank's exposure to cyber threats. It implies that as NBS improves its defenses and implements stronger strategies, its vulnerability of successful attacks is perceived to lessen, leading to a more secure environment. This is consistent with the goal of cybersecurity maturity, where enhanced capabilities lead to better risk mitigation (Scott et al., 2022).

4.7 Regression Analysis

Regression analysis was conducted to determine the extent to which the independent variable (Effectiveness of Cyber Risk Strategies) predicts the dependent variable (Exposure to Cyber Risks). This analysis helps understand the predictive power of cyber risk management effectiveness on the perceived exposure to cyber risks.

4.7.1 Model Summary and ANOVA

The regression model was built to assess the influence of the Effectiveness of Cyber Risk Strategies on the Exposure to Cyber Risks. The Model Summary provides an overview of the model's fit, while the ANOVA table indicates the statistical significance of the model.

Table 4.9: Regression Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.474[a]	.225	.219	.90369

a. Predictors: (Constant), ER

a. Predictors: (Constant), Effectiveness of Cyber Risk Strategies (ER)

b. Dependent Variable: Exposure to Cyber Risks (ECR)

Source: Primary data, 2025

The regression model, which includes the Effectiveness of Cyber Risk Strategies as a predictor, shows a moderate predictive relationship with the perceived Exposure to Cyber Risks. The multiple correlation coefficient (R) of 0.474 (the absolute value of the correlation) indicates the strength of the association between the two variables. The R-squared value of 0.225 signifies that 22.5% of the variance in the perceived Exposure to Cyber Risks can be explained by the perceived Effectiveness of Cyber Risk Strategies. The adjusted R-squared of 0.219 accounts for the number of predictors, confirming the model's explanatory power, albeit at a moderate level. This suggests that while cyber risk management effectiveness does influence the perception of risk exposure, other factors not included in this model also play a role.

Table 4.10: ANOVA Test Results

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	30.804	1	30.804	37.719	.000[b]
	Residual	106.166	130	.817		
	Total	136.970	131			

a. Dependent Variable: ECR

b. Predictors: (Constant), ER

a. Dependent Variable: Exposure to Cyber Risks (ECR)

b. Predictors: (Constant), Effectiveness of Cyber Risk Strategies (ER)

Source: Primary data, 2025

The ANOVA results show a highly significant F-statistic (F = 37.719) with a p-value of .000b. This indicates that the regression model is statistically significant, meaning that the perceived Effectiveness of Cyber Risk Strategies collectively predicts the perceived Exposure to Cyber Risks better than a model with no predictors. The low p-value confirms the statistical robustness of the model and the influence of cyber risk management effectiveness on the perception of risk severity within NBS.

4.7.2 Beta Coefficients and Interpretation

The standardized beta coefficients (β) indicate the strength of the relationship between the independent variable and the dependent variable, controlling for other variables in the model.

Table 4.11: Beta Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.675	.411		1.644	.103
	ER	-.692	.113	-.474	-6.142	.000

a. Dependent Variable: SCR

a. Dependent Variable: Exposure of Cyber Risks (SCR)

Source: Primary data, 2025

The regression analysis reveals that the perceived Effectiveness of Cyber Risk Strategies significantly predicts the perceived Exposure to Cyber Risks. The standardized beta coefficient (β) of -0.474 ($p < 0.000$) indicates a strong negative relationship. This means that for everyone standard deviation increases in the perceived effectiveness of cyber risk strategies, the perceived Exposure to Cyber Risks decreases by 0.474 standard deviations. This reinforces the correlation finding and suggests that a more effective cyber risk management approach directly leads to a reduction in perceived exposure, as improved defenses directly mitigate risks. It

implies that as NBS strengthens its cybersecurity, employees perceive a tangible decrease in the bank's vulnerability to cyber threats, leading to a more secure operational environment. This aligns with the concept of cybersecurity maturity, where a more mature organization is better at identifying and reducing its risks (Russell et al., 2022).

4.8 Discussion of Results

This section integrates the quantitative findings from the descriptive statistics, correlation and regression analyses with qualitative insights derived from the interviews conducted with key informants at NBS. The discussion is structured around the research objectives, providing a comprehensive understanding of cyber risk management effectiveness within the institution.

4.8.1 Key Cyber Threats and Vulnerabilities Faced by NBS

The quantitative data on cyber threats and vulnerabilities revealed a mixed perception among NBS employees. While ransomware and unauthorized data access were perceived as adequately addressed, phishing and malware infections remained significant concerns, with lower agreement on adequate protection. Insider threats and reliance on legacy systems also hovered in the neutral-to-concerned range. The qualitative interviews provided a deeper understanding of these perceptions. Key informants consistently highlighted phishing as a top and evolving threat. The IT Manager noted, "*Phishing attacks are relentless. Our employees are constantly targeted and despite training, some still fall victim. The sophistication of these emails makes them harder to detect*." This corroborates the quantitative finding of lower

perceived protection against phishing (Mean=2.70) and aligns with FireEye's (2022) observation that phishing attacks are highly targeted and sophisticated. Ransomware was also a significant concern, with a Risk and Audit Manager stating, "*Ransomware is a nightmare scenario. We've seen what it did to ZB Bank and it's a constant worry. Our focus is on backups and rapid recovery, but the threat is always there*." This supports the quantitative finding that ransomware threats are perceived as addressed (Mean=3.70) in terms of mitigation efforts.

Vulnerabilities stemming from legacy systems were a recurring theme in interviews. A Management representative explained, "*Our older systems, while functional, are not built with modern security in mind. Patching them is a constant challenge and they represent a significant attack surface.*" This reinforces the quantitative data showing a neutral perception regarding legacy systems (Mean=3.45) and aligns with studies emphasizing how outdated infrastructure increases vulnerability (Bachmann, 2020). Insider threats, both intentional and unintentional, were also frequently mentioned. A Compliance Officer stated, "*Human error is our biggest vulnerability. A single click on a malicious link can compromise our entire network. We also have to consider the potential for malicious insiders, especially given the economic climate*." This qualitative insight provides context to the neutral quantitative perception of insider threats (Mean=3.48), linking it to broader macroeconomic pressures as suggested by the Fraud Triangle Theory (Cressey, 1953), particularly in the Zimbabwean context of wage stagnation.

4.8.2 Effectiveness of Existing Cyber Risk Management Strategies at NBS

Quantitative results for the effectiveness of cyber risk strategies showed that incident response and training programs were perceived positively. However, the clarity of policies and procedures, adequacy of staffing and external collaboration received lower, more neutral scores. Qualitative data elaborated on these nuances. Regarding incident response, an IT employee commented, "*We have a clear plan for what to do when an incident occurs. We regularly drill it and everyone knows their role. This helps us contain breaches quickly*." This supports the high mean for incident response (Mean=3.82) and aligns with Davis et al.'s (2022) emphasis on effective incident response plans. Similarly, the perceived adequacy of cybersecurity training (Mean=3.79) was echoed by a Front Office employee: "*The training sessions are regular and cover common threats like phishing. They've made me more cautious*." This is consistent with KnowBe4's (2022) findings on the importance of awareness training.

However, the clarity and communication of cybersecurity policies (Mean=2.73) emerged as a significant area for improvement. A Risk and Audit employee stated, "*Our policies are comprehensive, but they are often too technical or buried in documents. It's hard for everyone, especially non-IT staff, to fully grasp them*." This qualitative feedback directly explains the low quantitative mean and suggests a gap in policy dissemination, which can undermine the effectiveness of even policies (Cisco, 2022). The adequacy of the cybersecurity team (Mean=3.45) was also a point of concern. A Management representative noted, "*We're always playing catch-up. The cyber threat landscape evolves so fast and finding skilled cybersecurity professionals in Zimbabwe is incredibly difficult. Our team is dedicated, but they are stretched thin*." This aligns with the broader challenge of IT skills emigration in Zimbabwe (Reserve Bank of Zimbabwe, 2022). Collaboration with external experts (Mean=3.30) was also

seen as needing improvement, with an IT Manager stating, "*We do engage some external consultants for specific assessments, but a more consistent information-sharing partnership with industry peers and law enforcement would be beneficial*."

4.8.3 Exposure to Cyber Risks Encountered by NBS

The analysis of cyber risk severity indicated that operational disruption and reputational damage were perceived as severe potential impacts. Financial losses, legal consequences, recovery costs, data compromise and systemic risk were perceived as less severe, falling into the neutral range. Qualitative insights provided context for these perceptions. The potential for operational disruption was a major concern for interviewees. A Management representative stated, "*If our systems go down, we cannot serve customers, we can't process transactions. That's immediate chaos and a massive hit to our daily operations*." This strongly supports the highest mean for operational disruption (Mean=3.55). Reputational damage was also a significant worry. A Front Office employee commented, "*Customer trust is everything in banking. If there's a major breach, people will lose faith in us and it will take years to rebuild that*." This aligns with the high mean for reputational damage (Mean=3.48) and the Ponemon Institute's (2020) findings on the long-term impact of breaches on trust.

The perception of financial losses (Mean=2.52) being less significant was surprising. An IT Manager explained, "*While direct financial theft is a concern, the indirect costs like recovery, legal fees and reputational damage often far outweigh the immediate cash loss. Perhaps people focus more on the direct theft, which we have controls against*." This qualitative explanation helps reconcile the lower quantitative mean for financial losses, suggesting a nuanced understanding of cost implications. Similarly,

the neutral perception of data compromise (Mean=3.03) was clarified. A Compliance Officer stated, "*We have robust data encryption and access controls. While a breach is always possible, we believe our measures would limit the extent of data compromise, though the regulatory implications remain severe*." This points to a perceived confidence in existing controls for data protection, even if the risk is acknowledged. The interconnectedness leading to systemic risk (Mean=3.15) was viewed as an industry concern rather than an immediate, direct threat to NBS alone, as articulated by a Risk and Audit Manager: "*Systemic risk is more of a national issue. We do our part, but it requires industry-wide collaboration*."

4.8.4 Proposed Enhanced Cyber Risk Management Strategies for NBS

The quantitative data on proposed strategies showed moderate support for most suggestions, with external collaboration and penetration testing receiving the highest agreement. Investing in advanced technologies received the lowest mean. Qualitative interviews provided context and additional recommendations. Strengthening collaboration with law enforcement and industry peers (Mean=3.55) was a highly supported strategy. An IT Manager emphasized, "*Sharing threat intelligence is crucial. We can't fight these sophisticated threats alone. We need to learn from others' experiences and contribute our own*." This aligns with Zhang et al.'s (2022) findings on the benefits of threat intelligence sharing. Regular penetration testing and vulnerability assessments (Mean=3.52) were also strongly advocated. A Risk and Audit Manager stated, "*We need to constantly test our defenses. Attackers are always finding new ways in, so we need to find them first*." This aligns with best practices for continuous security assessment (Basel Committee on Banking Supervision, 2022).

The lower perceived urgency for investing more in advanced threat detection and prevention technologies (Mean=2.58) was clarified by interviewees. A Management representative explained, "*While new tech is great, we first need to optimize what we have and ensure our basic hygiene is perfect. Also, the cost of advanced solutions, especially with foreign currency shortages, is a major barrier*." This highlights the practical constraints faced by financial institutions in Zimbabwe, where resource limitations can influence technology adoption, as noted by the Technology Acceptance Model (Davis, 1989) in the specific Zimbabwean context. Enhancing cybersecurity awareness training (Mean=3.39) was also a key recommendation. A Front Office employee suggested, "*Training needs to be more interactive and specific to the threats we actually face, like identifying fake payment requests*." This aligns with calls for improved cybersecurity awareness training (KnowBe4, 2022).

Other qualitative recommendations included Prioritizing a culture of security: A Compliance Officer stressed, "*It's not just about technology; it's about making security everyone's responsibility. We need a strong security culture*." This aligns with SANS Institute's (2022) emphasis on a security-aware culture. Another recommendation was about regular review and update of policies: An IT Manager noted, "*Policies become outdated quickly. We need a more agile process for reviewing and updating them to reflect new threats and technologies*." Clearer communication of risks to all levels: A Management representative suggested, "*Everyone needs to understand the 'why' behind security measures, not just the 'what.' This helps foster buy-in*."

The correlation analysis indicated a negative relationship between the effectiveness of cyber risk strategies and the perceived Exposure to Cyber Risks. This suggests that as NBS's strategies become effective, the perceived Exposure to Cyber Risks decreases,

indicating that improved defenses mitigate risks. The regression analysis further supported this, showing that effectiveness of strategies significantly predicts a reduction in perceived exposure. This implies that improving cyber risk management reduces the perception of risk, leading to a more secure environment and a clearer understanding that robust strategies directly lessen the likelihood and impact of cyber threats. This aligns with the concept of cybersecurity maturity models, where increased maturity leads to better risk identification and reduction (Scott et al., 2022).

4.9 Summary

This chapter analyzed data on cyber risk management effectiveness at NBS. A high response rate and diverse demographic profile characterized the participants, who demonstrated a high level of knowledge regarding NBS's cyber risk strategies. Descriptive statistics revealed mixed perceptions of cyber threats and vulnerabilities, with phishing and malware remaining concerns despite perceived strengths in addressing ransomware. The effectiveness of existing strategies was viewed as moderate, excelling in incident response and training but needing improvement in policy clarity. Perceptions of risk severity highlighted disruption and reputational damage as most impactful, while financial losses were less concerning. Proposed strategies favoured external collaboration and proactive testing, with less emphasis on advanced technology investment. Reliability tests confirmed high internal consistency and normality tests indicated non-normal data distribution, guiding the use of non-parametric correlation and regression analyses. Correlation and regression analyses showed a moderate negative relationship between the effectiveness of cyber risk strategies and the perceived Exposure to Cyber Risks, suggesting that improved strategies lead to a reduction in perceived exposure. Qualitative insights enriched these findings, providing crucial context for perceived threats, strategic effectiveness, risk severity and proposed improvements. Collectively, these findings show the necessity of a holistic cyber risk management approach at NBS, integrating technological and human factors while adapting to the evolving threat landscape in Zimbabwe's financial sector. Chapter 5 will discuss these findings, draw conclusions and offer recommendations.

CHAPTER 5 SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter provides an overview of the research study, integrating the findings presented in Chapter 4. It begins with a detailed discussion of the empirical results, linking quantitative data with qualitative insights to provide a holistic understanding of cyber risk management effectiveness at the National Building Society (NBS) in Zimbabwe. Following this, the chapter draws concise conclusions based on the study's objectives, outlines the practical, theoretical and methodological implications of the research and presents actionable recommendations for NBS and the broader financial sector. Finally, it identifies areas for future research to further enhance the understanding of cyber risk management in developing economies.

5.2 Discussion

This section integrates the quantitative findings from the descriptive statistics, correlation and regression analyses with qualitative insights derived from the interviews conducted with key informants providing an understanding of cyber risk management effectiveness at NBS.

5.2.1 Key Cyber Threats and Vulnerabilities Faced by NBS

The study's quantitative findings revealed a mixed perception among NBS employees regarding the cyber threats and vulnerabilities faced by the institution. While there was a relatively positive perception that ransomware attacks (Mean=3.70) and unauthorized access to sensitive data (Mean=3.64) were adequately addressed, concerns persisted regarding phishing attacks (Mean=2.70) and malware infections

(Mean=3.21). Qualitative interviews corroborated these quantitative results, with the IT Manager noting the "relentless" nature and "sophistication" of phishing attacks, leading to continued employee vulnerability despite training. This aligns with global financial sector trends where phishing remains a pervasive and costly threat. The perceived adequacy in addressing ransomware was explained by the Risk and Audit Manager, who highlighted a focus on "backups and rapid recovery" as key mitigation efforts, acknowledging it as a "nightmare scenario" and "constant worry" in the wake of incidents like the ZB Bank attack.

Furthermore, quantitative data indicated a neutral to slightly concerned stance on insider threats (Mean=3.48) and the vulnerabilities arising from reliance on legacy systems (Mean=3.45). Qualitative insights deepened this understanding; a management representative articulated that "older systems... are not built with modern security in mind," presenting a "constant challenge" for patching and a "significant attack surface." This reinforces the notion, consistent with Routine Activity Theory, that outdated infrastructure can become "chronically suitable targets." Insider threats, encompassing both human error and malicious intent, were described by a Compliance Officer as "our biggest vulnerability," particularly given Zimbabwe's economic climate, which could exacerbate pressure, opportunity and rationalization (Fraud Triangle Theory). The neutral perception regarding the effectiveness of cybersecurity measures against card cloning and fraud (Mean=3.27) is notable, especially given the documented increase in such incidents in Zimbabwe, suggesting a potential gap between perceived and actual protection in this area. The high standard deviations across all statements underscore the diverse opinions among employees, reflecting varying levels of awareness, departmental exposure and understanding of these threats.

5.2.2 Effectiveness of Existing Cyber Risk Management Strategies at NBS

The mean score for the effectiveness of cyber risk management strategies at NBS (Mean=3.49) suggested a neutral to slightly positive perception. Quantitative results indicated stronger agreement regarding NBS's incident response plan (Mean=3.82) and adequate investment in cybersecurity training and awareness programs for employees (Mean=3.79). Qualitative interviews supported these strengths; an IT employee confirmed a "clear plan for what to do when an incident occurs," with regular drills ensuring rapid containment. Similarly, a Front Office employee attested to the effectiveness of training sessions in making them "more cautious" against common threats like phishing. These findings align with the importance of incident response and continuous employee training in building cybersecurity resilience.

However, significant areas for improvement were identified. The lowest mean score was recorded for the clarity and communication of cybersecurity policies and procedures (Mean=2.73). A Risk and Audit employee explained that policies were often "too technical or buried in documents," making them difficult for non-IT staff to grasp, thereby undermining their effectiveness. This highlights a critical gap in policy dissemination, which can lead to non-compliance and increased vulnerability. The adequacy of the cybersecurity team (Mean=3.45) also emerged as a concern in qualitative interviews, with a management representative lamenting the difficulty in finding skilled professionals and the team being "stretched thin," reflecting the broader challenge of IT skills emigration in Zimbabwe. External collaboration with cybersecurity experts and organizations (Mean=3.30) was also perceived as needing strengthening, with an IT Manager suggesting a "more consistent information-sharing partnership with industry peers and law enforcement." These areas of neutrality or

slight disagreement, coupled with high standard deviations, indicate inconsistencies in how effectively these strategies are implemented and perceived across the workforce.

5.2.3 Severity of Cyber Risks Encountered by NBS

The assessment of cyber risk severity revealed a neutral to slightly concerned perception among respondents, with an overall mean of 3.12. The highest perceived severity was associated with operational disruption (Mean=3.55) and reputational damage (Mean=3.48). A Management representative emphasized that system downtime would lead to "immediate chaos and a massive hit to our daily operations," while a Front Office employee stressed that "customer trust is everything in banking," and a major breach would "take years to rebuild." These qualitative insights strongly support the quantitative findings, aligning with literature that highlights the significant intangible costs of cyber incidents for financial institutions.

Conversely, the potential for direct financial losses (Mean=2.52) received the lowest mean score, indicating a neutral or even slightly lower concern. An IT Manager clarified this, explaining that "indirect costs like recovery, legal fees and reputational damage often far outweigh the immediate cash loss," suggesting a nuanced understanding where direct financial theft might be perceived as more controlled. Other potential impacts, such as legal and regulatory consequences (Mean=3.15), recovery costs (Mean=2.94), sensitive data compromise (Mean=3.03) and systemic risk due to interconnectedness (Mean=3.15), all fell within the neutral range. A Compliance Officer noted confidence in existing controls for data protection, while the systemic risk was viewed more as an industry-wide concern rather than a direct threat to NBS alone. The consistently high standard deviations across these statements

highlight a wide divergence in opinions regarding the perceived severity of these risks, indicating varied understandings or experiences of potential impacts among employees.

5.2.4 Proposed Enhanced Cyber Risk Management Strategies for NBS

Quantitative data on proposed strategies for improving cyber risk management at NBS showed moderate support overall (Mean=3.28). Strengthening collaboration with law enforcement and industry peers (Mean=3.55) and regularly conducting penetration testing and vulnerability assessments (Mean=3.52) received the highest agreement. An IT Manager emphasized that "sharing threat intelligence is crucial" and that the bank "can't fight these sophisticated threats alone," while a Risk and Audit Manager stressed the need to "constantly test our defenses" to find weaknesses before attackers do. These findings align with best practices advocating for continuous assessment and collaborative intelligence sharing in cybersecurity.

However, investing more in threat detection and prevention technologies received the lowest mean score (Mean=2.58), indicating a neutral or slightly lower perceived urgency for this investment. A Management representative explained this, citing the need to "optimize what we have" first and highlighting the "major barrier" of cost, especially with foreign currency shortages in Zimbabwe. This constraint, influenced by the Zimbabwean economic context, impacts technology adoption, as implicitly suggested by the Technology Acceptance Model. Enhancing cybersecurity awareness training (Mean=3.39) was also a key recommendation, with a Front Office employee suggesting more "interactive and specific" training. Qualitative recommendations further included prioritizing a culture of security, regular review and update of policies

and clearer communication of risks to all levels of the organization. The high standard deviations for these proposed strategies indicate variation in opinions regarding their importance and feasibility, suggesting a lack of universal consensus on prioritization.

The correlation analysis revealed a moderate, negative relationship ($r = -.474$, $p < 0.01$) between the perceived effectiveness of cyber risk strategies and the perceived Exposure to Cyber Risks. This indicates that as the effectiveness of NBS's cyber risk management increases, the perceived exposure to cyber threats tends to decrease. The regression analysis further supported this, demonstrating that the perceived Effectiveness of Cyber Risk Strategies significantly predicts a reduction in the perceived Exposure to Cyber Risks ($\beta = -0.474$, $p < 0.000$). This implies that improving cyber risk management directly leads to a reduction in perceived exposure, fostering a more secure environment and aligning with the concept of cybersecurity maturity where enhanced capabilities lead to better risk mitigation.

5.3 Conclusions

Based on the findings and discussion, the following conclusions are drawn regarding cyber risk management effectiveness at NBS:

5.3.1 To establish the key cyber threats and vulnerabilities faced by the NBS.

NBS faces significant and evolving cyber threats, particularly from sophisticated phishing attacks and the persistent risk of ransomware. While some high-profile threats are perceived as adequately managed, vulnerabilities persist due to reliance on legacy systems and the inherent risk of human error, which is exacerbated by the broader socio-economic context. Card cloning and fraud also remain a concern, indicating areas where current protections may not fully align with the evolving threat landscape.

5.3.2 To evaluate the effectiveness of existing cyber risk management strategies at the NBS.

NBS demonstrates moderate effectiveness in its current cyber risk management strategies. The bank has established strengths in incident response planning and employee cybersecurity training. However, there are notable weaknesses in the clarity and communication of cybersecurity policies, the perceived adequacy of staffing within the cybersecurity team and the extent of collaboration with external cybersecurity experts. These areas require significant improvement to bolster the overall cybersecurity posture.

5.3.3 To assess the severity of cyber risks encountered by the NBS.

The most severe cyber risks perceived by NBS employees are the potential for operational disruption and significant reputational damage. While direct financial losses are viewed with less concern, the indirect costs associated with recovery, legal implications and loss of customer trust are recognized as substantial. The interconnectedness of systems also poses a systemic risk, though this is often viewed as a industry challenge rather than an immediate, direct threat to NBS alone.

5.3.4 To propose enhanced cyber risk management strategies tailored for the NBS.

To enhance cyber risk management, NBS should prioritize strengthening external collaboration with law enforcement and industry peers and regularly conducting penetration testing and vulnerability assessments. While investment in advanced technologies is acknowledged, its urgency is tempered by practical considerations like cost and the need to optimize existing defenses. There is also a clear need for more interactive and threat-specific cybersecurity awareness training, a stronger security culture and agile policy review processes.

5.4 Implications

5.4.1 Practical Implications

This study offers critical practical implications for NBS and other financial institutions in Zimbabwe. The findings highlight the necessity of improving policy communication and clarity, as well as addressing staffing and external collaboration gaps. For NBS management, the study underscores the importance of a holistic cybersecurity strategy

that moves beyond reactive measures to proactive defense, continuous assessment and a strong security culture. Policymakers can leverage these insights to develop more effective regulatory frameworks and support mechanisms that address the unique challenges of cyber risk management in a developing economy, considering economic constraints and skill shortages. Ultimately, strengthening cyber risk management contributes to enhanced financial stability, protects customer data and maintains public trust in Zimbabwe's financial sector.

5.4.2 Theoretical Implications

The study contributes to existing theoretical frameworks by applying them to the context of a developing economy's financial sector. It demonstrates how the Technology Acceptance Model (TAM) needs to account for infrastructural limitations (e.g., power disruptions) that undermine perceived ease of use, leading to workarounds that bypass security. The findings extend Routine Activity Theory by illustrating how legacy systems in resource-constrained environments become "chronically suitable targets" due to limited upgrade capabilities and IT skill emigration. Furthermore, the research enriches the Fraud Triangle Theory by highlighting how acute macroeconomic pressures, such as wage stagnation, can significantly amplify the "pressure" element, increasing insider threat risks. The study also implicitly challenges the direct applicability of forensic models like DFRWS, which assume stable infrastructure, by showing the need for context-specific adaptations in environments with frequent power cuts and data localization concerns. This research thus provides empirical evidence for refining these theories to better reflect the realities of cybersecurity in diverse global contexts.

5.4.3 Methodological Implications

The mixed-methods approach employed in this study, combining quantitative surveys with qualitative interviews, proved effective in providing a comprehensive understanding of cyber risk management effectiveness. The quantitative data offered statistical generalizability and identified trends, while the qualitative interviews provided rich contextual insights, explaining the "why" behind the quantitative perceptions and uncovering operational challenges. This triangulation of data enhanced the validity and reliability of the findings, demonstrating the value of mixed methods for complex organizational phenomena like cybersecurity. The study's careful consideration of non-normal data distribution and the subsequent use of non-parametric tests (Spearman's correlation) also serves as a methodological example for future research in similar contexts where data may not meet parametric assumptions.

5.5 Recommendations

Based on the findings, the following recommendations are presented to enhance cyber risk management effectiveness at NBS and for consideration by the financial sector in Zimbabwe:

5.5.1 Strategic and Governance Recommendations

Prioritize a Culture of Security: Senior management at NBS should actively champion and foster a pervasive security-aware culture across all departments. This involves consistent communication of cybersecurity's importance, leading by example and integrating security into performance appraisals for all employees, not just IT staff.

Invest in Policy Clarity and Dissemination: NBS should simplify its cybersecurity policies and procedures, ensuring they are easily understandable and accessible to all employees, regardless of technical background. Regular, interactive communication campaigns should be implemented to ensure widespread awareness and comprehension of these policies.

Strengthen External Collaboration: NBS should actively pursue and formalize partnerships with law enforcement agencies, industry peers and cybersecurity intelligence-sharing platforms. This proactive collaboration will enable timely threat intelligence exchange and the adoption of best practices to counter sophisticated cyber-attacks.

Integrate Cybersecurity into Business Processes: Cybersecurity considerations should be embedded from the outset in all new business processes, technology projects

and system developments. This "security by design" approach will reduce vulnerabilities inherent in new initiatives and minimize the need for costly retrofitting.

5.5.2 Operational and Technical Recommendations

Enhance Phishing and Malware Defenses: Given the persistent threat of phishing and malware, NBS should update and deploy advanced email filtering, endpoint detection and response (EDR) solutions and next-generation antivirus software. Regular simulated phishing exercises with targeted feedback should be a mandatory and ongoing training component.

Address Legacy System Vulnerabilities: NBS must develop a strategic roadmap for migrating away from or robustly securing legacy systems. This includes implementing virtual patching, network segmentation and strict access controls around older infrastructure to minimize their attack surface.

Optimize Cybersecurity Staffing and Skills: NBS should conduct a thorough assessment of its cybersecurity team's staffing levels and skill gaps. This includes investing in continuous professional development for existing staff, exploring partnerships with local universities for talent pipeline development and considering managed security service providers (MSSPs) to augment internal capabilities where necessary.

Implement Continuous Testing and Assessment: Regular and comprehensive penetration testing, vulnerability assessments and red teaming exercises should be conducted by independent third parties. These assessments should go beyond

compliance requirements to simulate real-world attack scenarios and identify exploitable weaknesses.

Develop Robust Data Loss Prevention (DLP) Strategies: NBS should implement and continuously refine a comprehensive DLP strategy to protect sensitive customer and institutional data. This includes deploying DLP tools, enforcing data classification policies and providing regular training on secure data handling practices.

5.5.3 Training and Awareness Recommendations

Tailored and Interactive Training

Move beyond generic cybersecurity awareness training to provide tailored, interactive and role-specific training programs. These programs should focus on practical scenarios relevant to each department's daily operations, emphasizing the "why" behind security measures.

Promote Reporting Mechanisms

Encourage employees to report activities without fear of reprisal. Establish clear, easy-to-use channels for reporting incidents and provide positive reinforcement for vigilant behaviour.

5.6 Suggestions for Further Research

Future research should improve our understanding of cyber risk management effectiveness in Zimbabwe's financial sector by:

Qualitative Exploration of Insider Threats: Conduct in-depth qualitative studies (e.g., focus groups, semi-structured interviews) with employees across various levels to explore the underlying factors contributing to insider threats, including socio-economic pressures and to identify effective mitigation strategies tailored to the Zimbabwean context.

Longitudinal Studies on Strategy Effectiveness: Implement longitudinal studies to track the long-term impact of specific cyber risk management strategies and investments (e.g., advanced technologies, training programs) on actual cyber incident rates and financial losses within financial institutions in Zimbabwe.

Comparative Analysis Across Financial Institutions: Conduct comparative studies across different types of financial institutions in Zimbabwe (e.g., commercial banks, microfinance institutions) to identify variations in cyber threat landscapes, risk management maturity levels and the effectiveness of different strategies.

Impact of Regulatory Frameworks: Examine the specific impact of Zimbabwean regulatory policies and frameworks on the adoption and effectiveness of cyber risk management practices within the financial sector, identifying areas for policy enhancement.

Role of Emerging Technologies: Investigate the feasibility, benefits and challenges of implementing emerging cybersecurity technologies (e.g., AI/ML for threat detection, blockchain for data integrity) within the Zimbabwean financial sector, considering local infrastructure and resource constraints.

Customer Perception of Cybersecurity: Explore customer perceptions of cybersecurity within Zimbabwean financial institutions, including their trust levels, awareness of risks and willingness to adopt secure practices, to inform public awareness campaigns.

References

Abdullah, S., et al. (2022). Understanding the adoption of cybersecurity technologies among SMEs: An extended TAM approach. *Journal of Cybersecurity, 8*(1), 102–115.

Akinsanya, I. O., et al. (2023). Board composition and cyber risk management practices in UK financial institutions. *Corporate Governance: An International Review, 31*(2), 345–362.

Al-Awadi, A., & Al-Mansoori, M. (2023). The DFRWS model and its implications for modern digital forensics. *Digital Forensics Review, 18*(2), 45–59.

Albrecht, S. W., et al. (2015). The Fraud Triangle: A comprehensive framework for understanding fraud. *Journal of Financial Crime, 22*(4), 392–410.

Al-Emran, M., et al. (2020). A survey of technology acceptance models in e-learning. *IEEE Access, 8*, 177560–177577.

Chen, T., et al. (2020). The role of perceived usefulness and ease of use in the adoption of cybersecurity technologies. *Information & Management, 57*(5), 103–115.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588–608.

Cressey, D. R. (1953). *Theft of the Nation: The Social Organization of Criminals.* Free Press.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative and mixed methods approaches* (4th ed.). SAGE Publications.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative and mixed methods approaches* (5th ed.). SAGE Publications.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.

DFRWS. (2001). *The DFRWS model: A framework for digital forensic investigation.* Digital Forensics Research Workshop.

Duc, A. N., Jabangwe, R., Paul, P., & Abrahamsson, P. (2017). Security challenges in IoT development: A software engineering perspective. In *Proceedings of the XP2017 Scientific Workshops* (pp. 11:1–11:5).

Financial Fraud Action Africa Report. (2022). *The impact of cybercrime on the African financial sector.*

Grant, C., & Osanloo, A. (2019). Understanding, selecting and applying a theoretical framework in dissertation research: From introduction to conclusion. *Canadian Journal for the Study of Practical Intelligence in Education, 11*(1), 48–69.

Gujarati, D. N. (2021). *Basic econometrics* (5th ed.). McGraw-Hill Education.

Hakim, C. (2013). *Research design: Successful planning for social, economic and political research.* Routledge.

Harkiolakis, N. (2020). *Quantitative research methods: From theory to publication.* Kogan Page.

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime: The investigation, prosecution and defense of a computer-related crime.* Routledge.

Hutchings, A., et al. (2021). Organizational routines and cybersecurity risk: A routine activity perspective. *Journal of Management Information Systems, 38*(3), 723–753.

Jiang, X., et al. (2022). Enhancing threat detection with machine learning in cyber risk management. *Journal of Financial Services Technology, 8*(2), 123–145.

Kaspersky Report. (2018). *Annual cybersecurity report.*

Kaur, R., Singh, S., & Gupta, P. (2022). Assessing cybersecurity risk management practices among Indian banks: A quantitative analysis. *International Journal of Bank Marketing, 40*(4), 789–805.

Koper, C. S., et al. (2020). Guardianship in cyberspace: Extending routine activity theory to online environments. *Journal of Research in Crime and Delinquency, 57*(4), 483–516.

Kothari, C. R. (2004). *Research methodology: Methods and techniques* (2nd ed.). New Age International.

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement, 30*(3), 607–610.

Legris, P., et al. (2003). Why do people use information technology? A critical review of the technology acceptance model. *Information & Management, 40*(3), 191–204.

Leukfeldt, E. R., et al. (2017). Understanding cybercrime victimization: A routine activity approach. *Crime and Delinquency, 63*(1), 66–87.

Liu, Y., et al. (2020). A systematic review of sampling methods in empirical studies. *Journal of Empirical Research, 15*(2), 234–256.

Lokanan, M. E. (2020). Beyond the fraud triangle: Expanding the analysis of factors contributing to corporate fraud. *Journal of Forensic Accounting Research, 5*(1), 1–23.

Marangunić, N., & Granić, A. (2015). Technology Acceptance Model: A systematic literature review. *Internet Research, 25*(3), 389–414.

Mintzberg, H., & Waters, J. A. (2018). Of strategies, deliberate and emergent. *Strategic Management Journal, 6*(3), 257–272.

Morales, A., et al. (2014). Fraud triangle theory: Implications for understanding fraud in organizations. *Journal of Business Ethics, 122*(1), 119–134.

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 16*(1), 1–13.

Patel, A., et al. (2022). Regulatory frameworks and cybersecurity preparedness: Evidence from Chinese banks. *Journal of Cybersecurity, 9*(1), 45–67.

Ponemon Institute. (2020). *Cost of a data breach report.*

RBI Report. (2020). *Report on trend and progress of banking in India.*

Reyns, B. W., et al. (2018). Routine online activities and risk for malware infection: A routine activity theory perspective. *Computers in Human Behavior, 82*, 192–199.

Roberta, S. (2013). DDoS attacks on U.S. banks: What happened and what's next. *CSO Online.*

Robson, C. (2014). *Real world research* (4th ed.). Wiley.

Salahuddin, M., et al. (2021). Phishing attacks: A fraud triangle perspective. *Computers & Security, 102*, 102142.

Sarker, S., et al. (2022). Compliance frameworks and cyber risk management in Australian financial institutions. *Australian Journal of Information Systems, 27*, 1–20.

Sennewald, C., et al. (2023). The effectiveness of artificial intelligence-powered cyber risk management systems in European financial institutions. *Journal of Financial Services Technology, 9*(1), 56–78.

Smith, J. (2019). *Understanding research design.* Routledge.

Smith, J., & Jones, A. (2024). Challenges of applying the DFRWS model in dynamic cybercrime environments. *Cybersecurity Studies, 3*(2), 98–112.

Thomson Reuters Accelus. (2018). *The cost of cybercrime.*

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. *Management Science, 46*(2), 186–204.

Wang, Y., et al. (2023). The impact of employee training programs on cyber risk management practices in US financial institutions. *Journal of Business Ethics, 184*(2), 345–362.

White, L., & Black, P. (2023). Managing electronic evidence: The role of eDiscovery models. *Journal of Legal Technology, 12*(1), 123–135.

World Economic Forum. (2020). *The global risks report 2020.*

Yar, M. (2005). The novelty of cybercrime: An assessment of the impact of the internet on crime. *Crime, Media, Culture, 1*(1), 75–92.

ZB Financial Holdings. (2024). *Ransomware attack report.*

Zimbabwe Information and Communication Technologies (ZICT) Report. (2020). *Cybercrime report.*

APPENDIX 1: Survey Questionnaire for NBS Employees

Dear Respondent,

My name is Charles Mapswayi and I am conducting research on "An Assessment of Cyber Risk Management Effectiveness in Zimbabwe's Financial Sector: A Case of National Building Society (NBS)." The study evaluates the effectiveness of cyber risk management approaches used by NBS to mitigate these growing threats. It identifies gaps and proposes enhancements to strengthen NBS's cybersecurity defences. Your insights will be valuable to this research. All responses will be treated with strict confidentiality and used solely for academic purposes.

Instructions:

1. Please do not write your name on this questionnaire.
2. Please respond by ticking [√] the appropriate box(es).
3. There is no right nor wrong answer; kindly provide answers for all questions.
4. Completion of this research questionnaire is a wilful act that should not be done in anticipation of receiving any thanksgiving.
5. Participants are free to stop participating at any given time.

Section A: Demographics and Background Information

A1. Indicate your age:

- 18 to 25 years [ ]
- 26 to 35 years [ ]
- 36 to 45 years [ ]
- Above 45 years [ ]

A2. Indicate your highest level of education:

- Ordinary Level [ ]
- Advanced Level/Certificate [ ]
- Diploma [ ]
- Bachelor's degree [ ]
- Master's degree [ ]
- Doctorate [ ]

A3. How long have you been working at NBS?

- Less than 1 year [ ]
- 1-5 years [ ]
- 6-10 years [ ]
- More than 10 years [ ]

A4. What is your department/role at NBS?

- IT [ ]
- Risk and Audit [ ]
- Compliance [ ]
- Front Office [ ]
- Management [ ]
- Other (please specify): _____

A5. How knowledgeable are you about NBS's cyber risk management strategies?

- Not knowledgeable [ ]
- Slightly knowledgeable [ ]
- Moderately knowledgeable [ ]
- Very knowledgeable [ ]
- Extremely knowledgeable [ ]

Instructions for Sections B, C, D and E

Please indicate your level of agreement with each statement using the following scale:
1 = Strongly Disagree 2 = Disagree 3 = Neutral 4 = Agree 5 = Strongly Agree

Section B: Key Cyber Threats and Vulnerabilities

This section assesses your perception of the key cyber threats and vulnerabilities faced by NBS.

Code	Statement	1	2	3	4	5
CT1	NBS is adequately protected against phishing attacks.					
CT2	The risk of malware infections on NBS systems is well-managed.					
CT3	NBS has effective measures in place to prevent unauthorized access to sensitive data.					
CT4	The threat of ransomware attacks on NBS is adequately addressed.					
CT5	NBS's systems are vulnerable to Distributed Denial of Service (DDoS) attacks.					
CT6	Insider threats (e.g., employees intentionally or unintentionally compromising security) are a significant concern at NBS.					
CT7	NBS's cybersecurity measures are effective in protecting against card cloning and fraud.					
CT8	The bank's reliance on legacy systems increases its vulnerability to cyber threats.					

Section C: Effectiveness of Existing Cyber Risk Management Strategies

This section assesses the effectiveness of the current cyber risk management strategies implemented at NBS.

Code	Statement	1	2	3	4	5
ER1	NBS's cybersecurity policies and procedures are clearly defined and communicated to employees.					
ER2	The bank conducts regular cybersecurity risk assessments to identify and address vulnerabilities.					
ER3	NBS has a robust incident response plan in place to effectively manage and mitigate cyber incidents.					
ER4	The bank invests adequately in cybersecurity training and awareness programs for employees.					
ER5	NBS effectively monitors and detects suspicious activities on its network and systems.					
ER6	The bank's cybersecurity measures are regularly updated to address emerging threats.					
ER7	NBS's disaster recovery and business continuity plans adequately address cyber-related disruptions.					
ER8	The bank's cybersecurity team is adequately staffed and equipped to handle cyber threats.					
ER9	NBS effectively collaborates with external cybersecurity experts and organizations to enhance its defenses.					
ER10	The bank's senior management provides strong support for cybersecurity initiatives.					

Section D: Severity of Cyber Risks

This section assesses your perception of the severity of cyber risks encountered by NBS.

Code	Statement	1	2	3	4	5
SR1	The potential financial losses resulting from a successful cyber-attack on NBS are significant.					
SR2	A major cyber incident could severely damage NBS's reputation and customer trust.					
SR3	A cyber-attack could disrupt NBS's critical operations and services.					
SR4	The legal and regulatory consequences of a cyber breach at NBS could be severe.					
SR5	The cost of recovering from a major cyber incident would be substantial.					
SR6	A successful cyber-attack could compromise sensitive customer data, leading to identity theft and fraud.					
SR7	The interconnectedness of NBS's systems with other financial institutions increases the potential for systemic risk from cyber-attacks.					

Section E: Additional Strategies for Improving Cyber Risk Management

This section explores potential strategies for improving cyber risk management at NBS.

Code	Statement	1	2	3	4	5
AS1	NBS should invest more in advanced threat detection and prevention technologies.					
AS2	The bank should enhance its cybersecurity awareness training programs to address specific threats and vulnerabilities.					
AS3	NBS should strengthen its collaboration with law enforcement agencies and industry peers to share threat intelligence and best practices.					
AS4	The bank should implement stricter access controls and authentication mechanisms to prevent unauthorized access to systems and data.					
AS5	NBS should regularly conduct penetration testing and vulnerability assessments to identify and address weaknesses in its cybersecurity defenses.					
AS6	The bank should develop a more robust data loss prevention (DLP) strategy to protect sensitive information from being stolen or leaked.					
AS7	NBS should establish clear metrics and reporting mechanisms to track the effectiveness of its cybersecurity measures.					
AS8	The bank should prioritize the integration of cybersecurity considerations into all business processes and technology projects.					
AS9	NBS should implement a zero-trust security model, where all users and devices are verified before being granted access to resources.					
AS10	The bank should establish a dedicated cybersecurity innovation team to research and implement emerging security technologies and practices.					

Thank you for your participation!

APPENDIX 2: Semi-Structured Interview Guide for Key Informants

Introduction

Thank you for agreeing to participate in this interview. My name is Charles Mapswayi and I am conducting research on the effectiveness of cyber risk management strategies at the National Building Society (NBS). Your insights as a key informant are invaluable to this research. The purpose of this interview is to gather in-depth information on the cyber risk management strategies, challenges and potential improvements at NBS. The interview will take approximately 30-45 minutes. Your responses will be kept confidential and used solely for academic purposes. You are free to decline to answer any question and may withdraw from the interview at any time. Do I have your consent to proceed?

Interview Questions:

A. Key Cyber Threats and Vulnerabilities

1. In your opinion, what are the most significant cyber threats currently facing NBS?

2. What specific vulnerabilities within NBS's systems or processes make it susceptible to these threats?

3. How has the threat landscape evolved over the past few years, and how has NBS adapted to these changes?

B. Effectiveness of Existing Cyber Risk Management Strategies

1. How would you describe NBS's approach to cyber risk management?

2. What specific strategies, policies, and procedures are in place to mitigate cyber risks?

3. How does NBS measure the effectiveness of its cyber risk management strategies?

C. Severity of Cyber Risks

1. What is your assessment of the potential financial impact of a successful cyber-attack on NBS?

2. How concerned are you about the potential reputational damage that could result from a cyber incident?

3. How prepared is NBS to respond to and recover from a major cyber incident?

D. Additional Strategies for Improving Cyber Risk Management

1. What additional measures could NBS take to strengthen its cyber risk management defenses?

2. How can NBS improve employee awareness and training to reduce the risk of human error?

3. What are the key challenges in implementing new cyber risk management strategies?

E. General Questions

1. What are the biggest challenges NBS faces in managing cyber risk?

2. Are there any emerging trends or technologies that you believe will significantly impact cyber risk management in the financial sector?

3. Is there anything else you would like to share about NBS's cyber risk management practices?

Thank you very much for your time and valuable insights!

National Building Society
A Registered Building Society

14th Floor Social Security Centre | Cnr Sam Nujoma Street & Julius Nyerere Way, Harare, Zimbabwe
|Tel (+263-242)700032, 700035, 700039, 700042 | Web:www.nbs.co.zw

02 April 2025

The ICT Director
National Building Society
SSC Centre, 14th Floor, Cnr J. Nyerere and 2nd Street
Harare.

To whom it may Concern

This letter seeks to authorise Charles Gwinyayi Mapswayi to conduct research on the **"An Assessment of Cyber Risk Management Effectiveness in Zimbabwe's Financial Sector: A Case of National Building Society (NBS)."**

Charles is employed within the society as a National Sales Manager and this research is in the best interest of the bank. Please feel free to assist him in any way possible while maintaining the highest form of integrity, confidentiality and secrecy which the Society must adhere to.

Yours Sincerely,

For and on Behalf of National Building Society

.....

Bianca Mahoso

Head Digital Channels

"Investing in Africa's future"
AFRICA UNIVERSITY RESEARCH ETHICS COMMITTEE (AUREC)

P.O. Box 1320 Mutare, Zimbabwe, Off Nyanga Road, Old Mutare-Tel (+263-20) 60075/60026/61611 Fax: (+263 20) 61785 Website: www.africau.edu

Ref: AU4043/25

3 November, 2025

CHARLES GWINYAYI MAPSWAYI
C/O Africa University
Box 1320
MUTARE

RE: An Assessment of Cyber Risk Management Effectiveness in Zimbabwe's Financial Sector: A Case of National Building Society (NBS).

Thank you for submitting the above-titled proposal to the Africa University Research Ethics Committee for review. Please be advised that AUREC has reviewed and approved your application to conduct the above research.

The approval is based on the following.

a) Research proposal

- **APPROVAL NUMBER** AUREC 4043/25
  This number should be used on all correspondence, consent forms, and appropriate documents
- **AUREC MEETING DATE** NA
- **APPROVAL DATE** November 3, 2025
- **EXPIRATION DATE** November 3, 2026
- **TYPE OF MEETING**: Expedited
  After the expiration date, this research may only continue upon renewal. A progress report on a standard AUREC form should be submitted a month before the expiration date for renewal purposes.
- **SERIOUS ADVERSE EVENTS** All serious problems concerning subject safety must be reported to AUREC within 3 working days on the standard AUREC form.
- **MODIFICATIONS** Prior AUREC approval is required before implementing any changes in the proposal (including changes in the consent documents)
- **TERMINATION OF STUDY** Upon termination of the study a report has to be submitted to AUREC.

AFRICA UNIVERSITY
RESEARCH ETHICS COMMITTEE (AUREC)
APPROVED
P.O. BOX 1320, MUTARE, ZIMBABWE

Yours Faithfully

MARY CHINZOU
FOR CHAIRPERSON
AFRICA UNIVERSITY RESEARCH ETHICS COMMITTEE