

BINDURA UNIVERSITY OF SCIENCE EDUCATION

TOWARDS LEADERSHIP ACCOUNTABILITY AND CYBER RISK GOVERNANCE FRAMEWORK IN THE FINANCIAL SERVICES SECTOR IN ZIMBABWE

BY

CLEMENCE CHIKOMBINGO

B250382A

A DISSERTATION SUBMITTED TO THE BINDURA UNIVERSITY OF SCIENCE EDUCATION IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR A MASTER OF SCIENCE DEGREE IN LEADERSHIP AND CORPORATE GOVERNANCE, GRADUATE SCHOOL OF BUSINESS

BINDURA, ZIMBABWE

JUNE 2026

APPROVAL FORM

The undersigned certify that they have read and recommended to Bindura University of Science Education (BUSE) for acceptance a Dissertation entitled **"Towards leadership accountability on cyber risk governance in the Financial Services Sector in Zimbabwe"** by **Clemence Chikombingo (B250382A),** in partial fulfilment of the requirements for a Master of Leadership and Corporate Governance Degree.

Student Name: Clemence Chikombingo (**B250382A**) Signature: ……Date: 28/06/2026

Supervisor Name: Dr Joseph Mupokosera II Signature:  Date: 28/06/2026

Program Coordinator Name: Dr M. Matambo Signature:  Date: 24.06.2026

External Examiner Name: …….. Signature: …… Date: ……..

RELEASE FORM

NAME OF AUTHOR: CLEMENCE CHIKOMBINGO

STUDENT NUMBER: B250382A

TITLE OF DISSERTATION: TOWARDS LEADERSHIP ACCOUNTABILITY ON CYBER RISK GOVERNANCE IN THE FINANCIAL SERVICES SECTOR IN ZIMBABWE.
BY CLEMENCE CHIKOMBINGO (B250382A).

DEGREE: Master of Leadership and Corporate Governance

YEAR DEGREE AWARDED: 2026

Permission is hereby granted to the Bindura University of Science Education Library to produce copies of this dissertation for private, scholarly, or scientific research purposes. The author reserves other publication rights for the dissertation or extensive extracts from it to be printed or otherwise reproduced without the author's written permission.

Signature: **Date: 28/6/2026**

Permanent Address: 682 Mazowe Valley Park, Mazowe

E-mail: clemchiko@gmail.com

Cell Number: +263786170667

DECLARATION FORM

I, CLEMENCE CHIKOMBINGO Student Reg Number B250382A, do hereby declare that this dissertation is a result of my own investigation and research, except to the extent indicated in the acknowledgments, bibliography, references, and comments included in the body of the report, and that it has not been submitted in part or in full for any other degree to any other university.

Signature……..… Date: 28/06/26…

DEDICATION

To God—whose grace, faithfulness, and strength sustained me through every season of this journey.

To my loving family: my husband and fatherhood, and especially my spouse, whose love, prayers, and steadfast support helped me persevere when the road felt long and the work felt heavy.

To my lecturers and mentors, thank you for your guidance, instruction, and encouragement throughout this dissertation.

With humility and gratitude, I dedicate this work in trust that it will honour God and bless others in ways I cannot yet imagine.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to the many people and sources of support that made this dissertation possible. First and foremost, I thank God for His grace, faithfulness, and strength throughout this journey. He has sustained me through every season of challenge and every moment of progress.

I am also deeply grateful for my loving family. As a husband and the father of three wonderful boys, I have been reminded daily of the importance of love, responsibility, and perseverance. I recognize the sacrifice it takes to continue striving for goals while balancing the demands of family life. To my spouse: thank you for your unwavering support, prayers, and encouragement. Your partnership and kindness have helped carry me when the workload felt heavy and when the path seemed long. I am truly grateful for the love and stability you have provided throughout this process.

I would also like to acknowledge my lecturers for their guidance, instruction, and academic mentorship. Thank you for the knowledge you shared, the constructive feedback you offered, and the encouragement you provided throughout my study. Your dedication to teaching and your commitment to excellence have played a significant role in shaping both my understanding and my confidence as I completed this dissertation.

Finally, I dedicate this work with humility and gratitude, trusting that it will bring honour to God and serve others in ways far beyond what I can yet imagine.

ABSTRACT

This study examines the role of leadership accountability in strengthening cyber risk governance within the financial services sector in Zimbabwe. The increasing digitisation of financial services has heightened exposure to cyber threats, revealing limitations in governance approaches that rely primarily on technical controls. The study aims to analyse existing cyber risk governance frameworks, evaluate leadership involvement, identify organisational constraints, and develop a context-specific framework to enhance governance effectiveness. A mixed methods research design was adopted, combining quantitative data collected through questionnaires and qualitative insights from interviews with professionals in financial institutions. The findings indicate that while cyber risk governance frameworks are generally established and aligned with organisational strategy, their implementation remains inconsistent. Leadership involvement, particularly in decision-making and resource allocation, was found to be limited. Additionally, organisational constraints such as financial limitations, skills shortages, and cultural factors significantly affect governance effectiveness. The study concludes that leadership accountability is a critical determinant of effective cyber risk governance. It proposes a context-specific framework that integrates governance structures, leadership engagement, organisational capacity, and environmental adaptation. The study contributes to both theory and practice by emphasising the need for leadership-driven governance approaches to enhance cybersecurity resilience in Zimbabwe's financial services sector.

Keywords: Cyber Risk Governance, Leadership Accountability, Cybersecurity: Financial Services Sector, Zimbabwe

Table of Contents

APPROVAL FORM ..... **i**

RELEASE FORM ..... **ii**

DECLARATION FORM ..... **iii**

DEDICATION ..... **iv**

ACKNOWLEDGEMENTS ..... **v**

ABSTRACT ..... **vi**

KEYWORDS: ..... **vi**

List of Figures ..... **xiii**

List of Tables ..... **xiii**

1 CHAPTER 1: INTRODUCTION AND BACKGROUND **1**

1.1 Introduction 1

1.2 Background of the study 1

1.3 Problem Statement 4

1.4 Research Objectives 4

1.4.1 Primary objective 4

1.4.2 Secondary objectives 4

1.5 Research questions 5

1.6 Justification of the Study 5

1.7 Expected Contribution 6

1.7.1 Theoretical Contribution 6

1.7.2 Methodological Contribution 6

1.7.3 Practical Contribution 6

1.8 Research delineation 7

1.9 Structure of the Dissertation 7

1.10 Chapter Summary 8

2 CHAPTER 2: LITERATURE REVIEW 9

2.1 Introduction 9

2.2 Theoretical Framework 9

2.2.1 Socio-Technical Systems Theory 9

2.2.2 Enterprise Risk Management Theory 10

2.2.3 Agency Theory and Accountability Mechanisms 11

2.2.4 Leadership Theory and Accountability in Cyber Risk Governance 12

2.2.5 Integrated Theoretical Framework and Study Relevance 13

2.2.6 Composition and Operational Environment of Zimbabwe's Financial Services Sector 14

2.3 Cyber Risk in Financial Services 16

2.3.1 Nature and Evolution of Cyber Threats 17

2.3.2 Digital Transformation and Expanding Attack Surfaces 18

2.3.3 Cyber Risk as a Systemic and Governance Issue 19

2.3.4 The Socio-Technical Nature of Cyber Risk 19

2.3.5 Human Factors and Organisational Vulnerabilities 20

2.4 Cyber Risk Governance 21

2.4.1 Conceptual Foundations of Cyber Risk Governance 22

2.4.2 Governance Frameworks and Models 23

2.4.3 Leadership and Accountability in Cyber Risk Governance 24
2.4.4 Structural and Operational Challenges 25
2.4.5 Towards Adaptive and Integrated Governance Approaches 26
2.5 Leadership Accountability 26
2.5.1 Theoretical Foundations of Leadership Accountability 27
2.5.2 Leadership Roles in Cyber Risk Governance 28
2.5.3 Leadership Accountability and Organisational Culture 29
2.5.4 Challenges in Leadership Engagement 30
2.5.5 Leadership Accountability in the Zimbabwean Context 31
2.6 Conceptual Framework 31
2.7 Chapter Summary 34
3 CHAPTER 3: RESEARCH METHODOLOGY 35
3.1 Introduction 35
3.2 Research Philosophy 35
3.2.1 Pragmatism 36
3.3 Research Approach: Mixed Methods Approach 37
3.4 Research Design 38
3.4.1 Survey Design 39
3.4.2 Case Study Design 39
3.5 Target Population and Sampling 40

3.5.1 Population definition for this study 40

3.5.2 Selection of population 40

3.5.3 Sample size 41

3.6 Sampling Methods and Techniques 42

3.6.1 Systematic Random Sampling Design (Survey) 42

3.6.2 Purposive Sampling Design (Interviews) 42

3.6.3 Questionnaires 43

3.6.4 Interview Guide 44

3.7 Data Collection Procedure 45

3.8 Data Analysis 45

3.8.1 Quantitative Data Analysis Techniques 46

3.8.2 Qualitative Data Analysis 47

3.9 Validity and Reliability 47

3.10 Trustworthiness 48

3.11 Ethical Considerations 48

3.12 Chapter Summary 49

4 CHAPTER 4: DATA PRESENTATION, ANALYSIS, INTERPRETION AND DISCUSSSION 50

4.1 Introduction 50

4.2 Response Rate (Analysis) 50

4.3 DEMOGRAPHIC DATA ANALYSIS 51

4.3.1 Age Distribution 51
4.3.2 Gender 52
4.3.3 Educational Qualification 52
4.3.4 Position 53
4.3.5 Type of Institution 54
4.3.6 Profile of Interview Participants 55
4.4 Descriptive Analysis Measures 56
4.4.1 Analysis of Cyber Risk Governance Frameworks in the financial sector 56
4.4.2 Analysis of leadership involvement 58
4.4.3 Analysis of Context-Specific Cyber Risk Governance 63
4.5 Inferential Analysis 64
4.5.1 Variable Definition 64
4.5.2 Reliability Testing 65
4.5.3 Reliability Statistics 66
4.6 Regression Analysis 66
4.6.1 Model Summary 66
4.6.2 Anova 67
4.6.3 Coefficients 68
4.7 Application of the Findings to Education 5.0: A Heritage-Based Approach 69
4.8 Chapter Summary 72

5 CHAPTER 5: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS 73
5.1 Introduction 73
5.2 Summary of Findings 73
5.3 Conclusions 74
5.4 Recommendations 75
5.5 Proposed Framework 76
5.6 Areas for Further Study 77
REFERENCES 78
APPENDIX 1: QUESTIONNAIRE 83
APPENDIX 2: INTERVIEW GUIDE 85
APPENDIX 3: SIMILARITY REPORT 86
APPENDIX 4: AI DETECTION REPORT 87
APPENDIX 5: ETHICAL CLEARANCE LETTER 88

List of Figures

Figure 2.1: Conceptual Framework 32

Figure 4.1:Age Distribution 51

Figure 4.2: Gender 52

Figure 4.3: Education 53

Figure 4.4: Position 54

Figure 5.1: Proposed Framework 76

List of Tables

Table 4-1: Response Rate 50

Table 4-2 Type of Institution 54

Table 4-3: Profile of Interview Participants 55

Table 4-4: Analysis of Cyber Risk Governance Frameworks 57

Table 4-5: Analysis of leadership involvement 59

Table 4-6: Analysis of Organisational Constraints 61

Table 4-7: Analysis of Context-Specific Cyber Risk Governance 63

Table 4-8: 4Variable Definition 65

Table 4-9: Reliability 66

Table 4-10: Regression Model Summary 66

Table 4-11: Anova Analysis 67

Table 4-12: Regression Coefficients 68

CHAPTER 1: INTRODUCTION AND BACKGROUND

1.1 Introduction

This chapter introduces a study on leadership accountability for cyber risk governance in Zimbabwe's financial services sector, with the ultimate purpose of developing a Cyber Risk Governance and Leadership Accountability Framework suited to the sector's institutional and regulatory environment. While digitalisation has transformed the accessibility, efficiency and delivery of financial services, it has simultaneously increased financial institutions' exposure to evolving cyber threats. This growing risk raises concerns about whether cyber security can continue to be treated primarily as a technical responsibility rather than a strategic governance obligation requiring active board and executive leadership. The study therefore examines existing leadership accountability, governance practices and institutional gaps in order to inform a practical framework that clarifies leadership responsibilities, oversight mechanisms, reporting structures and accountability for cyber risk. Against this context, the chapter presents the background and research problem, followed by the research objectives and questions. It further explains the significance, scope and limitations of the research and concludes by outlining the structure of the dissertation.

1.2 Background of the study

The global financial services industry has seen massive changes in recent years based upon digitalization and the advancement of technology in regards to customer service, access to finance and efficiency. The development and adoption of mobile financial services, online trading platforms, electronic payment systems and digital banking platforms have dramatically changed how financial services companies do business and how consumers gain access to those services. While these technologies have improved access and service quality, it has opened up new avenues of cyber attacks against financial organizations (Ambore et al., 2017).

The increase in cybercrime is becoming one of the most serious risks facing the world today. In terms of frequency, sophistication and financial impact on businesses globally, cybercrime has grown at an alarming rate, specifically affecting financial services companies (Sharma et al., 2021). Financial services companies are among the largest targets of cyber criminals because of the large amounts of money they handle and the vast amount of information they

keep about each customer (Kikuchi & Okubo, 2019). As much as banks use state-of-the-art technologies like firewalls, authentication mechanisms, encryption methods and security frameworks to prevent cyber attacks, cyber attacks continue to grow in numbers indicating that using technology alone will never solve the problem of managing cyber-risk (Herrera, 2021).

This continues to demonstrate that managing cyber-risk has evolved beyond being a mere technical issue to a major governance issue. Cyber-risk governance involves how organizations create a structure or framework for governing cybersecurity issues consistent with organizational goals (Bongiovanni et al., 2024). Strong governance requires transparency of accountability, clear-defined roles, and active participation from all levels of the organization including board members and senior executives (Falco et al., 2021).

Many organizations have yet to establish their own appropriate cyber governance, however, there are several instances of organizations establishing primary cyber responsibilities on Information Technology departments with senior level leaders and boards excluded from such responsibility (Herrera, 2021). Without the participation of senior-level leaders and boards within an organization, senior leadership and boards cannot provide the strategic direction or provide adequate oversight to ensure that all parties accountable for cyber risks are held so (Bongiovanni et al., 2024).

The importance of leadership accountability in managing risk has emerged as one of the most critical factors in successful risk management. While having systems and controls represents part of what constitutes risk management, it is merely one aspect. Successful risk management also involves how leadership behaves, makes decisions ethically, and creates and maintains an organizational culture (Campbell, 2015). The virtues exhibited by senior-level leaders including integrity, foresight, and responsibility, directly impact how organizations perceive and respond to risk (Campbell, 2015) thus indicating that governance frameworks which do not have sufficient leader accountability will fail to manage cyber risks.

Cybersecurity is a socio-technical issue; thus, understanding the interplay of technology, people, and organizational processes is essential in developing successful cybersecurity strategies. Human factors include behavior, awareness, and decision-making in both creating and preventing cyber-incidents (Falco et al., 2021). Therefore, cybersecurity success is

dependent not just on technical control measures but on senior-leadership inspired behavioral/cultural modifications (Ambore et al., 2017).

Moreover, given the dynamic nature of cyber threats poses further challenges to governance frameworks. Governance frameworks are often too inflexible to quickly respond to changing risks due to rigid structures, ambiguity around roles/responsibilities, and lack of flexibility (Bongiovanni et al., 2024). Thus, there are greater demands for more adaptable/integrated governance frameworks that emphasize leadership engagement/accountability throughout the entire organization (Bongiovanni et al., 2024).

Although cyber-risk governance has become recognized as a top-level strategy priority area there is limited academic literature on the role of leader accountability influencing governance outcomes in particular in developing countries. Most current literature reviews focus on technical solutions/governance frameworks broadly applicable to all types of organizations while providing little focus on the leader-dimension/its effect on efficacy of cyber-risk management (Campbell, 2015).

Within Zimbabwe's financial services sector there has been rapid transformational growth via mobile financial services/electronic payments (Chundu et al., 2025). This transformation has resulted in a substantial improvement in inclusive financial services/accessibility for previously un-banked individuals (Maphosa, 2024). However, the expanded dependence on digital platforms increases exposure to cyber-threats/risks as the integration of financial services creates vulnerability to cyber threats (Mutanda & Chrispen, 2023).

The development of effective cyber risk governance has been impeded by challenges that include changing regulatory environments, resource limitations and the varied nature of the level of cybersecurity maturity amongst financial institutions. Additionally, leadership accountability for cyber risk governance is also an area which has seen little development with most organisations having no clearly established roles or responsibilities for executives and boards of directors (Bongiovanni et al., 2024) creating a gap between the increasingly high level of cyber risk and their ability to manage it effectively. Therefore, this research aims to bridge the gap identified above through investigating the role of leadership accountability in cyber risk governance within the financial services industry in Zimbabwe so as to contribute to better practice and enhanced organisational resilience.

1.3 Problem Statement

Cyber security risks have increased dramatically for financial service companies as a result of their increased use of technology, which they now operate within increasingly frequent, complicated and constantly changing threat environments. Although there have been significant investments into advanced cyber security systems, the continued occurrence of cyber attacks highlights that it is unlikely to be possible to solely rely on technological tools to mitigate cyber security risks; therefore, both governance and leadership will play an important role in controlling cyber security risks. Unfortunately, cyber security continues to be primarily focused on technical activities with little involvement from executive-level leaders or board members and as a consequence, cyber security is poorly strategically overseen and does not reflect the organisation's risk appetite (Bongiovanni et al., 2024). Additionally, the definition of leadership accountability in relation to cyber risk governance is also very poor in many cases leading to confusion around who is responsible for the governance of cyber risk and therefore hindering coordinated action. As Campbell stated (2015) leadership characteristics such as integrity, forward thinking and risk consciousness are essential to effectively manage risks and at present are inadequately highlighted in current governance frameworks. Similarly in Zimbabwe, the accelerated adoption of digital banking has exacerbated existing issues related to the lack of clarity in regards to leadership accountability and therefore has weakened the ability of its banks to effectively govern cyber security risks.

1.4 Research Objectives

The study is driven by the following primary and secondary objectives:

1.4.1 Primary objective

The purpose of this study is to examine the role of leadership accountability in shaping cyber risk governance within the financial services sector in Zimbabwe, to develop a context-specific framework to enhance governance effectiveness.

1.4.2 Secondary objectives

1. To analyse the existing cyber risk governance frameworks in selected financial institutions in Zimbabwe

2. To evaluate the effectiveness of leadership involvement in cyber risk governance among the financial institutions in Zimbabwe.
3. To examine key organisational factors constraining leadership accountability in cyber risk governance in the financial sector in Zimbabwe.
4. To develop a context-specific leadership accountability framework that strengthens cyber risk governance in Zimbabwe's financial services sector

1.5 Research questions

This study is driven by the following research questions:

1. What are the existing cyber risk governance frameworks in selected financial institutions in Zimbabwe?
2. How effective is leadership involvement in cyber risk governance among financial institutions in Zimbabwe?
3. What organisational factors constrain leadership accountability in cyber risk governance within the financial services sector in Zimbabwe?
4. How can a context-specific leadership accountability framework be developed to strengthen cyber risk governance in Zimbabwe's financial services sector?

1.6 Justification of the Study

Cyber risk is now an inevitable risk to all financial institution's; however, currently, there remains a large emphasis on the technological aspect of managing cyber risk as opposed to understanding the role of leadership. The motivation behind this research is the growing need to understand how senior management accountability (i.e., leadership) affects the ability of financial institutions to effectively manage their cyber risks in light of the rapidly expanding use of digital financial services. Although most major financial institutions have spent considerable amounts of money implementing different types of cyber security solutions (e.g., firewalls, intrusion detection systems, etc.) there are very few that have adequately considered the decision-making processes, organizational structure, and the behavior of individuals who hold senior management positions as they relate to the implementation of these solutions. The Zimbabwean banking sector is also a good example of this issue due to its heavy reliance on digital platforms and mobile financial services. Thus, increasing senior management accountability provides an opportunity for banks to be able to more effectively mitigate risk through coordination and strategy. This research will therefore extend existing knowledge

related to technical solutions that address cyber security problems by examining the "human" or "governance" aspects of cyber security which have thus far received much less attention.

1.7 Expected Contribution

This study is expected to contribute to knowledge and practice in a meaningful way by addressing gaps in how cyber risk governance is understood and applied.

1.7.1 Theoretical Contribution

The study will build upon previous work and extend our knowledge of Cyber Risk Governance by examining how leadership can be held accountable for effective governance. A number of studies have examined technical solutions such as controls (for example) or broad governance structures, but few if any, have focused on the impact of leadership behaviours, decision making and responsibilities on the effectiveness of governance. The study will provide an integrated view of governance (structures) and accountability (culture).

1.7.2 Methodological Contribution

The study's methodology will provide an approach for assessing the governance of cyber risk which combines the assessment of leadership accountability with governance analysis. To facilitate this approach the study has adopted a qualitative research strategy to allow for an exploration of actual organisational practices and processes in the financial services industry; thereby providing a practical means of identifying how governance is practiced as opposed to solely theoretical. A qualitative approach also provides potential for future studies using similar approaches in other sectors or in developing countries.

1.7.3 Practical Contribution

The study will identify best practice recommendations for Financial Institutions to enhance their Cyber Risk Governance Practices. Additionally, it is anticipated that the proposed Leadership Accountability Framework (LAF) will provide an outline on how roles and responsibilities should be defined and decision making processes established. Therefore, this research may provide Financial Institutions with a means to transition from reactive responses to Cyber Threats to Proactive Strategic Management of Cyber Risk. It is possible that the

results of this study could also be used by Regulators and Policymakers when establishing or enhancing Governance Expectations for the sector.

1.8 Research delineation

This research is limited to the information security culture of financial services firms in Zimbabwe. Four of the eighteen banks currently operating in the country will be selected as case studies. The exact case studies have not yet been decided upon and they will not revealed given the sensitivity of both the financial services firms and the subject matter of information security. The study will be performed in the Harare Metropolitan province in Zimbabwe, where the researcher has acquaintances in the financial services sector. The latter will make it easier for the researcher to access the intended respondents.

1.9 Structure of the Dissertation

This dissertation is organised into five chapters, each addressing a specific aspect of the study on leadership accountability in cyber risk governance within the financial services sector in Zimbabwe.

Chapter 1: Introduction

This chapter provides the background to the study, outlines the research problem, objectives, and research questions. It also discusses the significance, scope, and structure of the study.

Chapter 2: Literature Review

This chapter reviews relevant theoretical and empirical literature on cyber risk, governance, leadership accountability, and information security culture. It identifies gaps in existing knowledge and develops the conceptual and theoretical framework guiding the study.

Chapter 3: Research Methodology

This chapter explains the research philosophy, design, population, sampling techniques, data collection methods, and data analysis procedures. It also addresses issues of reliability, validity, and ethical considerations.

Chapter 4: Data Presentation, Analysis and Discussion

This chapter presents and analyses the collected data using both quantitative and qualitative methods. The findings are interpreted and discussed in relation to the research objectives and existing literature.

Chapter 5: Summary, Conclusions and Recommendations

This chapter summarises the key findings, draws conclusions, and provides recommendations. It also presents the proposed framework and suggests areas for further research.

1.10 Chapter Summary

In this chapter, an overview was provided of the study focusing on leadership accountability in cyber risk management within the financial service sector in Zimbabwe. A need for strong governance has been identified to effectively counter the increased cyber threats that are becoming a part of the financial institutions' digital transformation. Background to the study was provided; the study problem was stated as well as the gap(s) related to leadership accountability were emphasized. Finally, the Research Objectives and Key Questions to be used to guide the research were described.Furthermore, the significance, scope, and limitations of the study were discussed. Finally, the structure of the dissertation was outlined to provide a clear roadmap for the study. Overall, the chapter established the foundation for the subsequent analysis and discussion in the research.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

Beginning with a review of the most appropriate current research on leadership accountability and cyber risk governance in the Financial Services Sector this chapter provides an overview of some key ideas, theories, and research-based findings that will be used as background to understand the context of the study. First, it explores cyber risks and how they affect financial service firms. Second, it examines various governance models or frameworks that can help lead organizations through challenges related to their cyber risks. Third, it describes the cultural aspects of information security; identifies what are considered the most important success factors in creating a strong information security program; and assesses the impact of previous work that has created standards for cybersecurity. Finally, the chapter examines several theoretical frameworks (socio-technical systems; enterprise risk management; agency theory; and leadership theory) that have been applied in similar contexts. The final section of the chapter presents a conceptual model based on these theoretical frameworks and prior research.

2.2 Theoretical Framework

To have a clear picture of cyber risk governance across all financial sectors with particular focus in Zimbabwe, it is important to use the appropriate theoretical models which will help us understand how organizations take advantage of technology, govern technology, and ultimately govern technology as part of their overall complex environment. Cyber risk governance has several dimensions beyond being just a technical issue. The development of effective cyber risk governance involves many factors including the interaction of organizational structure, leadership, and behavior (Ciriello et al., 2024) along with the systems and technologies used.

This research uses an interdisciplinary theoretical model based upon socio-technical system theory, enterprise risk management, agency theory, and leadership theory. Together, these theories create a solid base for analyzing how accountable leaders influence cyber risk governance. Nevertheless, although each of the theories provides useful insights into cyber risk governance, there are some limitations that require an integrated and contextualized approach.

2.2.1 Socio-Technical Systems Theory

Theories of socio-technical systems (STS) define organizations as systems consisting of interconnected social and technical components that should work together to provide optimum organization function (Thomas, 2024; Appelbaum, 1997). In particular, the STS concept is very relevant to Cyber Security because many cyber threats emerge through a combination of technical weaknesses and by way of human behavior (Ciriello et al., 2024).

Furthermore, the use of STS provides evidence of the necessity to focus on the development of a "whole" approach toward cyber risk management and governance. The theoretical basis for the development of this whole approach requires that there be synchronization between people, processes, and technologies. This synchronization further emphasizes the significance of organizational culture, user behavior, and system design to successful cyber security outcomes (Yurtseven & Buchanan, 2013). Leadership accountability is significant within this paradigm because leaders are ultimately accountable for ensuring that the investment made in technologies aligns with their organizational practice and behavioral expectations.

That being said, STS theories have several limitations when attempting to apply them to this research project. For example, STS theories emphasize the alignment of the interactions between social and technical aspects of organizations but do not place emphasis on organizational governance structure and accountability mechanisms. Furthermore, while STS theories describe the relationship between leaders and followers they do not clearly outline the various types of leadership roles that exist nor do they explain how leadership accountability is enforced within organizations. Finally, while STS theories assume that all organizations can obtain maximum alignment between their social and technical components, it would appear that this assumption may not always hold true in organizations with limited resources (e.g. Zimbabwe) (Maphosa, 2024).

2.2.2 Enterprise Risk Management Theory

Enterprise Risk Management (ERM) offers an enterprise-wide framework for risk identification, assessment and management aligned with organizational goals/objectives (Anton & Nucu, 2020; Ahmad & Teo, 2024). The key characteristics of ERM include

integrating risk management into strategic decision making and promoting inter-functional coordination among all areas of an organization.

Within the realm of Cybersecurity, ERM highlights the need to treat cyber risk as a strategic risk issue rather than simply a technical issue (Bongiovanni et al., 2024). Frameworks such as the Three Lines Model support this integration through defining roles and responsibility among Operational Management, Risk Oversight and Independent Assurance Functions.

Although ERM has many positive attributes it also has several shortcomings when compared to this study. One major shortcoming is that ERM typically focuses on formal structures and processes, whereas there are fewer resources devoted to behavioral or cultural issues related to cybersecurity. In addition, ERM assumes an organization's level of maturity and available resources. For example, organizations located in developing countries like Zimbabwe may not have sufficient resources or maturity to effectively implement ERM (Mutanda & Chrispen, 2023).

Another potential drawback of ERM is that it can be difficult to adapt to the changing landscape of cyber threats because traditional ERM approaches to risk management are usually rigid and static. An additional shortcoming is that ERM does not specifically address leadership accountability, including what role leader behavior plays in influencing effective governance. Based on these shortcomings, the authors believe that there will be opportunities to incorporate/combine other theoretical perspectives with ERM.

2.2.3 Agency Theory and Accountability Mechanisms

The authors go further to point out several limitations of agency theory. According to them, agency theory assumes that the primary motivation of an agent is personal gain. Therefore it fails to identify the important roles that "trust", "cooperation" and "shared responsibilities" can play in achieving successful relationships between principals and agents. Agency theory focuses primarily on the formal mechanisms of corporate governance and largely ignores the many informal aspects of governance including organizational culture and behavior from the CEO down. Finally, the authors argue that agency theory views governance as generally static rather than dynamic; therefore, it cannot be expected to help organizations respond to changes in risk or rapidly evolving cyber threats. This would appear to be especially true for smaller

countries like Zimbabwe where there are often significant legal and regulatory obstacles to effective governance. As such, it appears reasonable that the authors propose integrating agency theory with other theoretical perspectives to better understand behavioral and context-based dimensions of good corporate governance.

In addition, Al-Faryan (2024) states that "agency theory explains how firms create internal controls to reduce uncertainty related to decision making".

2.2.4 Leadership Theory and Accountability in Cyber Risk Governance

Transformational Leadership Theory emphasizes the inspirational and motivational aspects of transformational leadership and the promotion of a shared vision for cybersecurity among employees. As mentioned by Slapnicar et al. (2023), this type of leadership fosters an environment where innovation is encouraged.

Ethical Leadership Theory addresses ethical concerns in organizations through integrity, transparency, and responsibility. Campbell (2015) has indicated that these characteristics are necessary for establishing accountability and trust.

In the area of cyber risk governance, both transformational and ethical theories highlight the importance of leaders' roles in developing strategic objectives, resource allocation, and creating a culture of security awareness. The behaviors of employees are directly influenced by leaders; thus, it is imperative that cybersecurity be integrated into organizational policies (Bongiovanni et al., 2024).

Despite the many benefits associated with transformational and ethical leadership theories, there are several limitations. Both theories have been criticized for focusing primarily on the traits/behaviors of individual leaders while providing little consideration to the impact of organizational structures/governance systems. Therefore, neither theory adequately explains how accountability is embedded within organizations. Further, many assume that all leaders possess sufficient knowledge/capacity to understand/manage their organization's cyber risk posture; however, this is not always the reality. Bongiovanni et al. (2024) reported that many leaders lack technical experience/knowledge and therefore cannot become involved in cyber risk management decisions.

Finally, neither theory considers the integration of cybersecurity into larger governance models nor do they account for contextual elements that affect governance, including regulatory and economic environments. Thus, it appears that both theories need to be combined with other theoretical models to create a comprehensive framework for managing cyber risk.

2.2.5 Integrated Theoretical Framework and Study Relevance

The use of four different theories (agency theory, enterprise risk management, leadership theory and socio-technical system theory) will provide a base line for investigating Cyber Risk Governance by providing a range of perspectives and also pointing out limitations that are identified when integrating these different theories.

While the application of socio-technical systems theory identifies how the interplay between human and technology-based elements interact with one another it fails to address the issue of accountability. Similarly, enterprise risk management establishes established processes to govern organizations' risks; however, it has limited ability to account for both behavioral and contextual influences. Agency theory addresses issues of accountability and governance but fails to consider cultural or dynamic influences. Finally, leadership theory describes the manner in which leaders exert influence over others but does not establish a complete model to describe both the structure of governance and the complexity of technology used within this structure.

Thus, this integrated conceptual framework presents relevance to the rapidly developing digital financial service industry in Zimbabwe. In particular, the framework presents the opportunity to investigate how leadership accountability may be enhanced as part of the process of creating effective governance systems and organizational resilience. Therefore, the combined use of agency theory, enterprise risk management, leadership theory and socio-technical systems theory provides a comprehensive and critically informed basis for studying leadership accountability in Cyber Risk Governance. Additionally, while each individual theoretical perspective provides value to understanding Cyber Risk Governance, the limitations associated with each represent a rationale for employing an integrated framework that reflects the complexity inherent to Cyber Security challenges.

2.2.6 Composition and Operational Environment of Zimbabwe's Financial Services Sector

Zimbabwe's financial services sector is a heterogeneous and increasingly technology-dependent system comprising commercial banks, building societies, microfinance institutions, insurance companies, pension funds, mobile network operators (MNOs) and emerging financial technology (fintech) providers. Commercial banks remain central to financial intermediation through deposit mobilisation, credit provision and payment services, while MNOs and fintech firms have progressively altered the structure of financial service delivery through mobile money, digital payments and technology-enabled financial products. This transformation reflects wider international developments in which fintech firms increasingly complement, compete with and reshape traditional financial intermediaries through data-driven and digitally mediated business models (Sharma et al., 2021). In Zimbabwe, these developments are particularly significant because high mobile-phone penetration, combined with limitations in conventional banking infrastructure, has created conditions in which digital platforms have become important channels for expanding financial access.

The sector nevertheless operates within a demanding environment shaped by the interaction of macroeconomic instability, regulatory complexity and accelerated digitalisation. Zimbabwe's historical experience of hyperinflation, currency changes, liquidity constraints and declining confidence in formal financial institutions has required financial institutions to continually adjust their operating models. Digitalisation has consequently become more than a mechanism for improving convenience; it has developed into an important means of sustaining service delivery, expanding customer reach and maintaining competitiveness under volatile economic conditions. Remote banking, mobile payment platforms and internet-based financial services have improved accessibility and operational efficiency, but the same technologies have enlarged the cyber-attack surface of financial institutions. This creates a central governance tension: the technologies upon which institutions increasingly depend for resilience and growth simultaneously expose them to operational disruption, financial loss, data breaches and reputational damage. Poor governance and inadequate risk-management practices may

intensify these exposures and increase institutional vulnerability to operational and reputational losses (Chitruju, 2025).

This tension is becoming more pronounced as financial institutions adopt cloud computing, Artificial Intelligence and Internet of Things technologies. Although these technologies provide opportunities for innovation and more responsive financial services, they introduce interconnected vulnerabilities that cannot be addressed adequately through technical controls alone. Phishing, malware, unauthorised access and compromise of sensitive customer information demonstrate how cyber incidents can migrate rapidly from information technology problems into matters affecting institutional continuity, regulatory compliance and stakeholder confidence. Effective cyber resilience therefore depends upon the interaction of technological safeguards, organisational risk-management practices and regulatory oversight (Michael, 2026).

The Reserve Bank of Zimbabwe and the Insurance and Pensions Commission occupy important regulatory positions within this environment by overseeing compliance and contributing to financial-system stability. However, the speed at which digital technologies and cyber threats evolve creates difficulties for regulatory systems that must continually respond to new technologies, business models and information-security risks. This challenge is compounded by shortages of specialised cybersecurity expertise, constrained institutional resources and the loss of skilled personnel through migration. Consequently, cyber-risk exposure cannot be understood simply as the product of technological weakness; it is also shaped by institutional capacity, regulatory responsiveness, organisational culture and the priority accorded to cybersecurity within strategic decision-making.

Leadership accountability therefore becomes particularly important. Cybersecurity has increasingly shifted from being predominantly an Information Technology function towards becoming an enterprise governance concern requiring active participation by boards and senior executives. Governance approaches such as the “Five Lines of Accountability” demonstrate

the importance of clearly allocating responsibility for identifying, escalating, monitoring and responding to cyber risk (Slapničar et al., 2023). Conversely, organisations that concentrate cybersecurity responsibility primarily within Information Technology departments may create accountability gaps between technical risk management and executive governance (Bongiovanni et al., 2024). Within Zimbabwe's financial services sector, this distinction is significant because institutional concentration and increasing digital interconnectedness mean that serious cyber failures may have consequences extending beyond an individual organisation to customers, counterparties and wider financial-system confidence.

Zimbabwe's financial services environment therefore presents a distinctive intersection of digital dependence, economic uncertainty, institutional capacity constraints and evolving cyber threats. The central issue is no longer simply whether financial institutions possess adequate cybersecurity technologies, but whether leadership structures provide clear ownership, oversight and accountability for the risks generated by digital transformation. This study is situated within that governance problem. It examines how cyber-risk responsibilities are understood, allocated and exercised at leadership level and uses these insights to inform the development of a **Cyber Risk Governance and Leadership Accountability Framework** appropriate to Zimbabwe's financial services sector. Such a framework shifts the analytical focus from cybersecurity as predominantly technical protection towards cyber resilience as an institutional governance responsibility involving leadership accountability, regulatory alignment, organisational capability and strategic oversight..

2.3 Cyber Risk in Financial Services

The financial sector is one of the most exposed areas to cybercrime due to its dependency on technology, the large sums of money involved with it, and also due to the fact that this area holds a tremendous amount of sensitive customer information. In addition to being one of the most frequently targeted groups by cyber crime hackers, the financial institution group is one of the largest groups to be victimized by cyber crimes because these hackers can profit from the theft of customer's funds, and/or access sensitive customer data or even disrupt the systems used by consumers, businesses and governments (Herrera Luque et al. , 2021; Falco et al. , 2021)

In recent years, technology has increasingly influenced the way financial service providers operate. Digital development has therefore changed what was once seen as a purely technological issue into a strategic problem that threatens both organizational resilience and financial stability through poor governance (Slapničar et al., 2023; Bongiovanni et al., 2024).

Financial institutions have been creating new avenues for cyber attackers by using increasingly sophisticated digital products such as online banking and mobile payment applications, which have significantly improved efficiency and access to financial services. However, many of these same digital products also present new challenges for organizations seeking to protect against cyber threats. These new challenges cannot be addressed effectively with traditional risk management approaches (Peihani, 2022). Cyber risk is no longer contained to the level of an organization alone and can potentially spread throughout multiple levels of a complex financial system, thereby placing the overall economy at greater risk of collapse (Herrera Luque et al., 2021)

2.3.1 Nature and Evolution of Cyber Threats

Cyber threats facing the Financial Services Sector have increased in sophistication, variety and persistence. While traditional threats such as Malware and Phishing continue to be common-place, they have developed into newer and more sophisticated variants which incorporate Artificial Intelligence, Social Engineering and Automation (Thomas, 2024; Sharma et al., 2021).

As a result of this development, cyber-attackers can now exploit both technical vulnerabilities and human weakness. This is particularly difficult when attempting to detect and prevent them.

For example, Phishing Attacks have been increasingly targeted and personalising in nature. They use information that has been collected via social media and other means to trick victims. Ransomware attacks on the other hand, have increased significantly. Attackers will encrypt critical systems and demand money for the decryption key. As well as disrupting normal business operation, these types of attack can lead to the loss of sensitive information and subsequent damage to reputation and finances (Falco et al., 2021).

Insider Threats also pose a high level of risk. Employees who have access to sensitive information could either deliberately or inadvertently compromise an organisation’s security.

The research shows that the most common cause of security breaches still stems from human error. Therefore it is clear that behaviour and organisations play an important part in how effective an organisation's Cyber Security Strategy is (Ciriello et al., 2024).

The increasing complexity of cyber-threats mirrors the increasing sophistication of technology generally, such as Cloud Computing, Internet of Things, and Artificial Intelligence. While these technologies bring many advantages there are also greater risks than previously existed that need to be addressed through creative risk management techniques (Michael, 2026).

2.3.2 Digital Transformation and Expanding Attack Surfaces

Cyber risks associated with digital financial services have rapidly grown due to growing complexity. Digital payment services include mobile banking, e-wallets, etc. These have contributed greatly to expanding financial inclusion throughout emerging markets. In addition, they have introduced a number of entry points for cyber attacks and, therefore, a greater likelihood of a breach occurring. (Peihani, 2022; Ambore et al., 2017)

Due to an exponential increase in connected systems and platforms, this is becoming increasingly complicated. Banks often employ third party vendors, cloud computing and APIs. Each one introduces potential new avenues for vulnerabilities. Vulnerability in one element of a network can be devastating to all elements of a network. This emphasizes the need to implement holistic approaches to manage cyber risk. (Herrera Luque et al., 2021)

In addition, with an ever-growing reliance on working remotely and digital collaboration tools, organizational networks continue to grow and become more complex to secure. When employees are accessing systems from numerous devices at multiple locations, there is a significant opportunity for unauthorized access to systems and data breaches. New security architecture, such as zero-trust architectures, will likely become more prevalent. Zero-trust architectures emphasize the necessity of continuous verification and monitoring. (Falco et al., 2021)

Although digital transformation provides many benefits to banks and other financial institutions including improved competitiveness and sustainability, the major hurdle is finding balance between security and innovation. To maximize the potential of digital technologies,

organizations should ensure that their implementation does not minimize the risk of exposure but rather maximize the benefit. (Sharma et al., 2021).

2.3.3 Cyber Risk as a Systemic and Governance Issue

Cyber risk within the Financial Services Sector is increasingly being perceived by many as an issue that impacts upon the system rather than merely at an organizational level. As a consequence of this interconnectivity within the Financial Systems, a cyber incident occurring in one organization may cascade throughout the entire sector and potentially undermine financial stability (Herrera Luque et al. 2021).

A further consequence of adopting this systemic perspective is that there will be an increasing focus upon the development and implementation of Governance and Regulatory Frameworks. Regulators and Policymakers are now requiring Financial Institutions to develop and implement Comprehensive Cyber Security Strategies; to undertake Risk Assessments regularly; and to Report Incidents. Although Compliance with these regulatory requirements is important for organizations to demonstrate their commitment to addressing the dynamic nature of cyber threats it is unlikely to provide an effective solution to managing those threats (Slapničar et al. 2023)

The effectiveness of a Governance Structure relies heavily upon the active engagement and participation of Senior Management and Boards of Directors. This is because Leaders should ensure that Cyber Security is fully integrated into Organizational Strategy; Risk Management Processes; and Decision-Making Frameworks. Research indicates that Organizations with Stronger Governance Structures are generally better positioned to effectively Manage Cyber Risks and Respond to Incidents (Bongiovanni et al. 2024). In addition to the structure itself, Governance Frameworks also need to establish how Responsibilities will be Coordinated Across Different Functions within an Organization. The coordination of Responsibility for Cyber Risk Management across Multiple Stakeholders such as IT; Risk Management; Compliance; and Executive Leadership is critical. Failure to Coordinate Responsibly can lead to Gaps in Accountability and Ineffective Responses to Threats.

2.3.4 The Socio-Technical Nature of Cyber Risk

A new trend is developing that views cybersecurity within financial institutions as a socio-technical problem where technologies interact with people and business processes. The idea that you need to combine both the technical and social aspects to manage security has been discussed by some researchers since Appelbaum (1997), an early researcher who studied this topic. This combination of the two viewpoints is still present in the majority of today's research.

Although technology such as encryption, firewalls, intrusion detection systems, etc. Provides considerable protection for information assets including data, it needs to be used along with appropriate business practices and user behavior. For example, weak passwords, failure to keep software and/or hardware updated and susceptibility to phishing email scams will all potentially weaken even the most secure technology (Sharma et al., 2021).

A key element of the socio-technical view of cybersecurity emphasizes the need for integrated approaches that include addressing both the technical and social aspects of cybersecurity. Developing cyber related policies and procedures and creating cultures of cyber awareness will assist in supporting user behavior in relation to cybersecurity. Providing training and assistance to employees will help them understand how to protect against cyber threats. Designing systems that are user friendly and minimize the potential for mistakes or errors will reduce the risk of system misuse (Michael, 2026).

Finally, the socio-technical approach recognizes that cyber defense is an ongoing process. Organizations must continually adapt to changing cyber threats through updates to their technologies, processes and behaviors in order to maintain resilience.

2.3.5 Human Factors and Organisational Vulnerabilities

Human Factors play a substantial role in influencing Cybersecurity Outcomes within Financial Services. The actions/decisions made by employees, customers and leaders directly impact how well Security Measures function. Numerous studies have shown that human error is one of the primary causes of security breaches due to lack of awareness, inadequate training, or bad decision making (Thomas, 2024; Ciriello et al., 2024).

When employees unintentionally put organizations at risk through clicking on malicious links, providing sensitive information, or ignoring security procedures they increase exposure. There are instances where insider threats occur when employees intentionally commit malicious acts

against the organization such as theft of data or fraudulent activities. This highlights why it is so imperative for organizations to create and maintain a strong Information Security Culture that creates accountable behavior.

In addition to employee behavior, Leadership has a significant role in how organizations respond to cyber risks. Their decisions on budgeting for resources, developing policies and managing risk will determine whether the organization becomes stronger or weaker as a result of those decisions (Bongiovanni et al., 2024). Research indicates that Leadership involvement is required to create a culture of security throughout an organization and to ensure that cybersecurity is considered and implemented at every level of the organization.

Similarly, Customers represent another important aspect of the Cybersecurity Ecosystem. As Users of Digital Financial Products/Services, customer's behaviors can affect the security of systems/data. Examples include using weak passwords and/or not recognizing phishing scams which could allow hackers access to customer accounts exposing the institution to potential risk. Therefore, there is a necessity for organizations to develop awareness and education programs that extend beyond organizational boundaries.

2.4 Cyber Risk Governance

Cyber Risk Governance is now at the heart of how organizations manage their cyber security, especially in those industries which are highly dependent on digital systems and therefore face significant systemic risk, most notably in the Financial Services sector. Literature surrounding cyber risk governance has evolved to view it as a core component of an organization's strategy to integrate its organizational structure, processes, and leadership into a single framework to identify, manage, and align cyber risk with broader business objectives (Kikuchi and Okubo, 2019; Mohammed Alharbi, 2025). Unlike traditional views of governance focused solely on technical solutions or "cyber" domains, contemporary research emphasizes the importance of accountability, coordination, and decision making at various organizational levels (Slapničar et al., 2023; Bongiovanni et al., 2024).

In order to be effective in mitigating ever increasing cyber threats by both size and complexity, organizations will have to develop governance structures that are not only robust, but flexible enough to adapt to new and emerging cyber threats. Research conducted over the past seven

years (2019-2026) demonstrates a transition from a compliance-focused approach toward more integrated governance frameworks that include embedding cyber security within an organization's overall Enterprise Risk Management (ERM), strategic planning process (Falco et al., 2021; Sharma et al., 2021). This section provides a critical review of several fundamental components of cyber risk governance including: Frameworks, Leadership Roles/Responsibilities, Structural Challenges, and Adaptive Approaches.

2.4.1 Conceptual Foundations of Cyber Risk Governance

Cyber risk governance refers to all the means through which organisations control and determine cybersecurity activities. This includes policies and procedures for cybersecurity; roles of responsibility in terms of cybersecurity; structures that provide accountability in relation to cybersecurity; and formal and informal systems that enabling effective and consistent management of cyber risks across the entire organisation (Kikuchi & Okubo, 2019)

Recent literature emphasises that governance is about how cybersecurity can be incorporated into an organisational strategy. This involves including cyber risk assessments within decision making processses; ensuring that these risks are asssessed against business objectives; and allocating resources to manage those risks accordingly (Mohammed Alharbi, 2025).

Cyber risk governance is therefore closely linked to enterprise-wide risk management frameworks and corporate governance frameworks.

The evolution of cyber risk governance has been driven by changes in the cyberspace landscape generally. In the past, cybersecurity was generally viewed as a technical function under the oversight of information technology departments. However, given the impact that cyber incidents have on an organization's performance and reputation, cybersecurity has now become a strategic issue that requires executive level oversight (bongiovanni et al., 2024).

Increasingly, governance frameworks also take into account the cultural dimensions and behaviour of an organization. Study results suggest that effective governance requires not just formal structure but also a supportive organizational culture that promotes ethics, knowledge about security issues, and accountability (slapničar et al., 2023), highlighting the interdependence between governance and security culture.

2.4.2 Governance Frameworks and Models

The Three Lines Model is another of the models used to assist organisations to implement effective cyber risk governance. It has become perhaps the most universally accepted model and is frequently utilised by large and small organisations alike. The Three Lines Model divides an organisation's activities into three lines of defence; or rather, three lines of defence against potential cyber attacks. Each line provides a level of protection against potential cyber attacks through the identification of threats, the development of strategies to mitigate the identified threat(s), and the implementation of the mitigation strategy(ies) (Bongiovanni et al., 2024).

The first line of defence includes operational management. Operational management identifies and manages cyber risks on a daily basis. The second line of defence includes the risk management and compliance functions of the organisation. Risk management and compliance functions identify cyber risks and develop policies to protect against identified cyber risks. They also monitor adherence to established policies. The third line of defence includes the internal audit function. Internal audit functions perform an independent review of an organisation's governance processes.

Recently, there has been an extension to the three lines model including two additional layers of governance. These layers include executive management and board members. Executive management defines risk appetite, sets business objectives, and ensures accountability for both the execution of defined objectives and the overall direction of the company. Boards of Directors oversee all aspects of corporate operations including information security. This expanded view recognises that cybersecurity cannot exist independently from corporate governance (Slapničar et al., 2023).

There are other frameworks that can help organisations manage their cyber risk. There are several different types of frameworks available. One type includes those frameworks that rely upon international standards. International standard-based frameworks typically address four areas including risk assessments, policy creation/revision, incident responses, and ongoing improvements (Sharma et al., 2021). While these frameworks provide general guidance in each of these areas, it is unclear if they will be effective unless they are properly implemented by each organisation. Research has shown that while many organisations do possess at least one framework for managing their cyber risk, few are able to successfully utilise that framework.

Some common challenges facing organisations when attempting to convert their frameworks into actual practices include: a lack of clearly defined roles/responsibilities among stakeholders, inadequate funding for cyber risk related initiatives, and inadequate integration with existing organisational strategy (Falco et al., 2021). As such, frameworks need to be tailored to meet specific needs of individual organisations and/or environments in order for them to be successful.

2.4.3 Leadership and Accountability in Cyber Risk Governance

The involvement of senior executives and Board members, in developing an organisation's cyber risk governance, is paramount to its success. The tone from the top, the prioritisation of cybersecurity within organisational strategy, and the integration of cybersecurity into all aspects of the organisation are all underpinned by senior management. Studies have shown that leaders' accountability for managing cyber-risk will enable the development of effective governance. While it has been identified that allocating budgetary allocations, approving policies, etc., are important components of providing direction on how to manage cyber-risk; equally important is active participation in assessing, monitoring and enforcing compliance with established cyber-risk related policies and procedures (Slapničar et al., 2023). A visible commitment from senior managers demonstrates to both internal stakeholders and external parties the value placed on cybersecurity and directly affects how employees perform their duties.

Evidence does exist that shows varying levels of commitment to cyber security by senior managers. Many organisations delegate responsibility for implementing cyber security measures to their IT departments without much input from other senior managers (Falco et al., 2021), creating a disconnection between the operational management of cyber-risks and strategic decision making; therefore diminishing the effectiveness of governance arrangements.

Senior manager's accountability also entails defining clearly defined roles and responsibilities throughout the organisation. Without clarity regarding who is accountable for what aspect of cyber-risk, there exists ambiguity which creates vulnerabilities in the implementation of risk management strategies. Therefore, effective governance must include well-defined accountability mechanisms which mirror organisational structures and processes (Mohammed Alharbi, 2025).

Finally, senior managers must develop a culture of accountability and transparency within the organisation. Developing such a culture would encourage open communication concerning the existence or potential exposure of cyber-risks, allow employees to report incidents freely, support ongoing education and training activities. Such practices support the development of a more agile and resilient organisation.

2.4.4 Structural and Operational Challenges

Although there are many theoretical approaches to developing governance models, organizations still experience difficulty with implementing them. Two of the most common barriers to successful governance model implementation include; the assignment of responsibility for cybersecurity to an organization's IT department and the rapidly changing environment of cyber threats.

As a result of concentrating the role of Cybersecurity within the IT department, this results in a narrow focus on Cybersecurity as part of organizational strategy and therefore diminishes the ability to implement governance models effectively (Bongiovanni et al. 2024). Moreover, due to the evolving nature of cyber threats as technology evolves at an unprecedented rate and new types of attacks emerge regularly, it becomes increasingly challenging for organizations to continually update their governance structure. As policies and procedures related to Cybersecurity evolve, they require constant assessment and updates to remain relevant (Sharma et al. 2021).

In addition to these two challenges, complex organizational environments add complexity to the development of effective governance. Large organizations typically have multiple departments or business units that manage cyber risk which may lead to redundancy or overlap and inefficient use of resources. These issues may result in duplicated efforts, inconsistencies in practice, and lack of accountability for those responsible for managing cyber risk (Falco et al. 2021).

The existence of cross-border activities presents an additional challenge to developing effective governance especially in the Financial Services industry. Different countries have different regulations, laws, and technological standards that may present additional layers of complexity when developing effective governance. Organizations will need to balance navigating these

differences while maintaining consistency in their risk management practices across borders (Sharma et al. 2021).

2.4.5 Towards Adaptive and Integrated Governance Approaches

The shortcomings of traditional forms of governance have led many researchers to emphasize the need for new and adaptive ways to govern cyber risk. Traditional governance models are limited in their ability to adapt to the complexity and rapid changes occurring in the cybersecurity arena; therefore, they provide limited organizational flexibility and resilience.

Adaptive governance has become a prominent theme in research on cyber risk governance. Adaptive governance involves ongoing monitoring, learning, and adjustments to policy and practice based upon changing risks or threats. For organizations to engage in adaptive governance, they will need to establish investments in threat intelligence, data analysis, and feedback mechanisms to allow for decisions to be made quickly enough to be responsive to evolving threats.

Another component of governance is integration. Cyber risk governance should be an integral part of other organizational processes such as enterprise risk management, strategic planning, and performance management. By doing so, cybersecurity will be included in all aspects of organizational decision making.

In addition to being an integral part of organizational processes, information security culture plays a significant role in supporting adaptive governance. Organizations with a strong security culture foster an environment where employees are aware of cyber risk and accountable for mitigating it. Strong security cultures promote proactive behavior among employees which allows them to respond to emerging cyber threats.

Finally, the importance of collaboration and shared information is becoming increasingly recognized as a vital element of governance. To effectively combat common cyber threats and create cooperative responses, financial institutions, regulatory agencies, and industry associations must collaborate. Collaborative efforts to mitigate cyber threats improve the overall resiliency of the global financial system.

2.5 Leadership Accountability

Leadership Accountability as an Emerging Aspect of Cyber Risk Management

As organizations become more reliant on digital systems, there exists a growing need for leadership accountability as part of the successful cyber risk management process. Governance provides a structural framework for organizations to address cyber security issues, however, it is leadership who will ultimately implement the governance structure and hold individuals accountable in implementing these structures, and sustaining them over time (Auffret et al., 2017). The current body of research identifies that leadership accountability is now considered a key strategic element driving the success of an organization's cyber security efforts. In addition to leadership accountability being linked to executive involvement, organizational culture, and cyber risk management processes (Slapničar et al., 2023), Bongiovanni et al. (2024) also suggest this is driven by leadership accountability.

Cybersecurity as a Board-Level Issue

Over the past few years, the increased complexity and frequency of cyber threats have transformed what was once a technical issue into one that requires the attention of boards. Therefore, due to the necessity for all organizations to proactively manage their cyber risks through coordinated effort, leadership accountability has transitioned from optional to necessary.

2.5.1 Theoretical Foundations of Leadership Accountability

The different conceptualizations of the idea of accountability of leaders in terms of cybersecurity provide a basis on which we can look at the agency theory as one of the theoretical foundations. According to agency theory, there is a relationship between principal actors (such as shareholders) and agent actors (such as managers) where principals seek mechanisms to ensure their agents take action that benefits the parties who own the organization (Panda and Leepsa, 2017). The application of agency theory to the area of cybersecurity focuses on the problem of information asymmetry. Generally, technical personnel have specialized knowledge that non-technical personnel do not. Therefore, when technical personnel are able to develop or implement technology without adequate oversight from management, it can result in a lack of alignment in priorities, inadequate oversight and poor decision making (Cole and Schneider, 2020). Senior executive officers or Board Members

may under estimate potential cyber threats or not assign sufficient resources to address these threats due to their lack of understanding of the underlying technological complexity. Recent research has identified that in order to address the issue of information asymmetry, organizations should improve transparency, communications and reporting mechanisms. Leaders must have access to data and other forms of relevant and understandable information so they can make informed decisions regarding organizational cyber security issues (Al-Faryan, 2024). Some examples include developing KPIs (Key Performance Indicators), dash boards and reporting formats that convey strategic insights based on the translation of technical information into those strategic insights. Stewardship Theory also provides another lens on this subject and suggests that leaders are naturally inclined to make decisions that benefit their organization. In accordance with stewardship theory, accountability of leadership is demonstrated by establishing trust and shared responsibilities among all members of the organization in relation to cyber security (Slapničar et al., 2023).

2.5.2 Leadership Roles in Cyber Risk Governance

There has been research conducted into how effective or ineffective the strategies developed by organizations to implement their Cyber Security plans have been. The effectiveness of an organization's Cyber Security plan will depend upon many factors including; the type of industry the organization operates in, whether the organization is large or small, the type of employees working within the organization, and what level of budget was assigned to developing and implementing the Cyber Security plan. A study found that Cyber Security has become one of the most important issues facing business today as well as being a major threat to individual privacy. The article stated that companies need to take proactive measures when it comes to protecting themselves from cyber-attacks. In order for this to be successful, the organization needs to develop and implement a comprehensive and well-planned Cyber Security program.

The authors of this report state that there are four main areas where organizations should focus when developing their Cyber Security programs:

(1) Network security: Organizations need to protect all of their network devices such as routers, switches and firewalls. These are used to control who has access to the internal and external

networks and therefore limit potential entry points that could allow hackers to gain unauthorized access.

(2) Application security: All applications used throughout the organization need to be reviewed for security vulnerabilities prior to use. Once identified, patches need to be implemented immediately. If an application cannot be patched, it may need to be removed from service until a solution can be implemented.

(3) Data protection: Protecting customer information is critical. Companies need to protect their data through encryption, backup systems and other methods. Companies must also educate employees about proper use of company assets.

(4) Incident response: Organizations need to have a well-defined incident response process in place in case a cyber-attack occurs.

2.5.3 Leadership Accountability and Organisational Culture

Leadership is accountable within an organisation due to its direct relationship to organisational culture. The culture of a company is shaped by what employees believe and do based on the values and norms that a leader promotes. A key factor in developing a culture of accountability for cybersecurity is ethical leadership which has been described as being responsible, having integrity and being forward thinking (Campbell, 2015) .

Research from recent years indicates that it is important to have a well-established security culture in order to effectively manage cyber risk. Employees will be more inclined to follow the appropriate security procedures and comply with policies that relate to security when they know that leadership values cybersecurity and demonstrates this value through their actions (Bongiovanni et al., 2024). However, if leadership does not support cultural initiatives related to security then those initiatives may fail to be successful. In addition to influencing employee behavior and the success of cultural initiatives, leadership provides a means to foster open communication regarding risks, incident response and lessons learned which enhances organisational learning and resilience.

When employees feel that leadership holds them accountable for reporting problems and supporting ongoing improvements then they are more likely to report problems and adhere to

policies (Slapničar et al., 2023). In addition to accountability, leadership accountability relates directly to ethical matters concerning cybersecurity. As companies deal with greater volumes of sensitive information than ever before, leadership must establish that all security practices are compliant with ethics and protection of stakeholders. Examples include data privacy, confidentially, and the responsible use of technology.

2.5.4 Challenges in Leadership Engagement

Despite the identified value of leadership accountability in respect of cyber security, it appears that many organisations are experiencing limited leadership involvement within cyber security activities. A key barrier is the reliance upon technical experts when making decisions about cyber security. While technical competence will always be important, too much dependence on technical specialists will often prevent senior managers from becoming active participants in both strategy development and risk management discussions (Bongiovanni et al. 2024).

The dependency is frequently further complicated due to the inherent complexities surrounding cyber security. For example, executives may not have sufficient technical skills and understanding to comprehend all associated risks; therefore they may adopt a 'hands-off' attitude towards their role in governance. Consequently, cyber security may be viewed merely as a tactical/operational activity rather than a strategic focus area (Falco et al. 2021). Another factor that inhibits leadership accountability is the number of alternative strategic objectives that organisational leaders must simultaneously address. Examples include growth, innovation, profit, etc. The competing demands may lead to insufficient attention and resource allocation being made available for various cyber security-related initiatives (Sharma et al. 2021).

In addition, organisational structure can be another hindrance to leadership accountability. Within large or complex organisations, responsibility for cyber security can be fragmented across numerous departments and functions creating ambiguity, confusion and potential gaps in accountability. These structural arrangements can impede the effectiveness of governance arrangements (Slapničar et al. 2023). Finally, there may be cultural impediments which deter leadership participation. For example, if an organisation has no history of prioritising cyber security or has been resistant to change, then the leadership may find it difficult to implement effective governance mechanisms.

2.5.5 Leadership Accountability in the Zimbabwean Context

The significance of leadership accountability is apparent in the Zimbabwean financial service sector which has been rapidly transformed digitally and therefore exposed to many new cyber-risks. Mobile banking, digital payments and online financial services have all contributed to greater financial inclusion; however they have created new vulnerabilities (Maphosa, 2024) Financial institutions in Zimbabwe operate within a dynamic environment that includes limitations of available resources, changing regulatory frameworks, and varying degrees of maturity of cybersecurity processes (Mutanda & Chrispen, 2023). This dynamic environment may limit the establishment of an effective governance framework as well as rely upon reactive methods to address cybersecurity issues.

Therefore, in this particular context, the accountabilities of leadership will be pivotal in driving the organizational changes necessary to proactively manage cyber risks. Leadership will need to assess and prioritize technology investments, develop governance processes that align with local conditions, and understand the interdependencies of both technical and non-technical elements of the organization. Furthermore, leadership is instrumental in developing solutions to address skill gaps and capacity deficiencies. Developing the capacity of employees through investment in education and training will help create resilient organizations. In addition, collaboration with local regulatory agencies, national associations/industry bodies, or international entities may assist in developing effective methodologies for managing cyber security risks. Finally, the unique challenges presented by the Zimbabwean context highlight the importance of adaptability when implementing leadership accountability. The evolution of regulatory environments and the increasing sophistication of cyber threats require ongoing updates to strategy and practices. Therefore, there must be a long-term commitment to learning and innovation, as well as a focus on continuous improvement.

2.6 Conceptual Framework

The conceptual Framework is derived from the literature review and research objectives of the study as follows

The Independent Variable

- Leadership Accountability in Cyber Risk Governance

This is operationalised through four key constructs derived from the study objectives:

1. Cyber Risk Governance Frameworks
2. Leadership Involvement
3. Organisational Constraints
4. Context-Specific Framework Development

Dependent Variable

1. Effective Cyber Risk Governance

The four constructs collectively shape Leadership Accountability

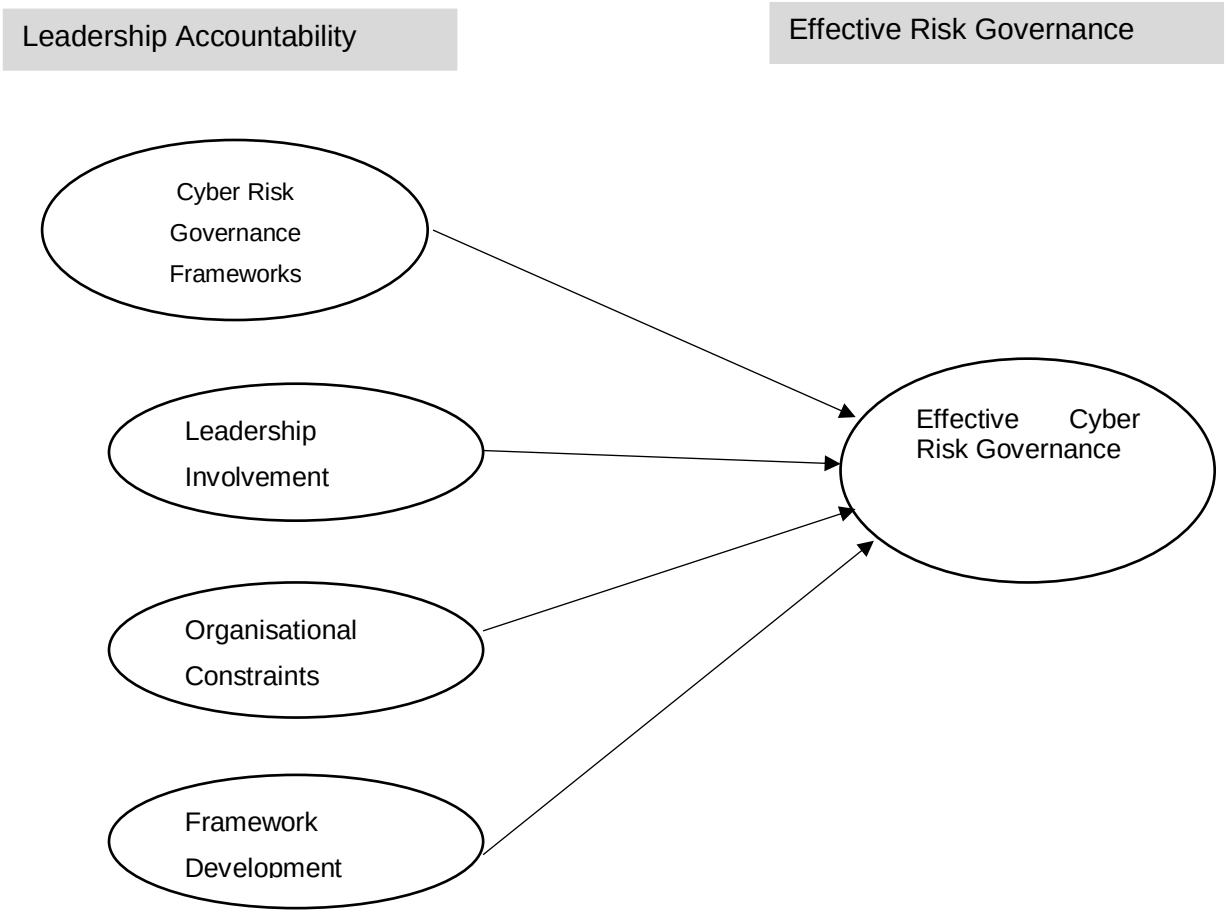


Figure 2.1: Conceptual Framework

The Cyber Risk Governance framework states that Leadership Accountability is the most important single driver to successful cyber risk governance within the Financial Services sector.

Leadership Accountability has been identified as the "link" where current governance frameworks are translated into action by organizations based on how a company interprets, implements and enforces their respective governance frameworks.

This framework identifies four key constructs that drive Leadership Accountability – existing governance frameworks, leadership involvement, organizational constraints and contextual adaptation.

Existing governance frameworks represent the formal structure, policy and process required to manage cyber risk. However, empirical evidence has demonstrated that the formalization of governance frameworks does not lead to successful outcomes if there is a lack of consistent and engaged leadership (Falco et al., 2021) . As a result, leadership involvement is recognized as an important factor to ensure cyber risk is incorporated into organizational strategy (Mohammed Alharbi, 2025).

Therefore, leadership involvement is identified as a critical factor in determining accountability. It affects decision making, resource allocations and oversight. Empirical evidence demonstrates that organizations with an active level of leadership participation in cybersecurity have greater likelihood of demonstrating good governance practices and improving resilience against cyber attacks (Sharma et al., 2021). On the other hand, a lack of leadership engagement results in fragmented governance arrangements and reactive responses to risk management (Bongiovanni et al., 2024).

The Conceptual Model is designed to provide empirical evidence supporting the primary assertion of the study—namely, that strengthening Leadership Accountability enhances Cyber Risk Governance within Zimbabwe's Financial Services Sector. The model creates an opportunity to assess the extent to which Leadership Accountability may be developed or expanded upon to improve Cyber Risk Governance through a systematic process. Furthermore, it serves as a foundation for developing a Context-Specific Framework addressing challenges in relation to the development of Cyber Risk Governance in Zimbabwe's Financial Services

Sector and therefore contributes to both Theory and Application of Knowledge in the field of Cybersecurity Governance.

The four Constructs of Organizational Constraints, Contextual Adaptation, Governance Approaches and Cyber Risk Governance are interdependent and serve as a structural base for defining Leadership Accountability and subsequently impact the Dependent Variable — namely, Effective Cyber Risk Governance. Effective governance encompasses improved risk detection, active threat mitigation, compliance with regulations and enhanced organizational resilience. Prior research has demonstrated that organizations with high levels of Leadership Accountability have the potential to successfully integrate their cybersecurity strategies with their organization-wide strategic objectives, effectively address emerging threats and maintain stakeholder trust (Bongiovanni et al., 2024; Slapničar et al., 2023).

In addition to providing direct support for the central claim made by this study regarding the positive relationship between increasing Leadership Accountability and improving Cyber Risk Governance in Zimbabwe's Financial Services Sector, the conceptualization also moves beyond merely technical solutions to develop a more comprehensive understanding of governance based on organizational behavior and situational factors. This conceptualization is consistent with existing research trends that view cybersecurity as a socio-technical/governance challenge requiring active and strategically aligned leadership engagement (Ciriello et al., 2024).

Ultimately, the conceptualization provides a structured approach to evaluate how Leadership Accountability may be strengthened to enhance Cyber Risk Governance. Moreover, it offers a platform to establish a Context-Specific Framework addressing specific issues associated with the establishment of Cyber Risk Governance in Zimbabwe's Financial Services Sector contributing to both Theory and Applicability of Knowledge in the area of Cybersecurity Governance.

2.7 Chapter Summary

Cyber risk leadership accountability in the financial services sector was the focus of this study. The authors describe cyber risk today as being much more complex and having the potential

for systemic disruptions greater than at anytime in history. This study will explore and identify various cyber risk governance frameworks and highlight the importance of a process-driven approach to cyber risk governance, clear definitions of role and responsibility among participants in the cyber risk governance processes, and participation by organizational leaders. Additionally, this research supports leadership accountability as a critical factor influencing effective cyber risk governance through theoretical models such as Socio-Technical Systems Theory (STST), Enterprise Risk Management (ERM), Agency Theory (AT), and Leadership Theory (LT). The study develops a conceptual model which indicates that leadership accountability is key to effectively managing cyber risk governance frameworks, particularly in the Zimbabwean financial service sector.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

This chapter sets out the methodology that was employed in this study. In the last chapter we presented an overview of the literature on Leadership Accountability and Cyber Risk Governance; and as part of our review we have indicated some of the principal gaps within this body of knowledge which motivated this research. This chapter describes the philosophical underpinnings of the research, its overall design, strategy, and methods by which the research objectives were pursued. Additionally it addresses the methodological approaches taken to obtain samples from which to collect data; how these data will be collected and analyzed; and issues related to the validity, reliability and ethics of both data collection and analysis. As such, the intention of this chapter is to provide a structured plan for implementing the research so that there is no ambiguity regarding how the research process has been carried out. The structure and transparency of the research process provides evidence of rigour in pursuing the aims and objectives of this study.

3.2 Research Philosophy

The term “research philosophy” represents a system of beliefs regarding what we know from our studies (Saunders et al. 2019) and how that knowledge is perceived. These beliefs influence

all phases of the research process including selecting a research design, selecting a method for conducting the research and interpreting the results of the study (Burrell & Morgan, 2019). There are four main areas of belief or assumption as it pertains to research philosophy. Ontology represents the nature of reality. Epistemology is concerned with how knowledge is developed. Axiology is related to the value(s) involved in developing the knowledge used during the research process (Saunders et al. 2019).

For this particular study the primary concern will be with the development of knowledge through the lens of an epistemological perspective. The reason is this study is attempting to develop knowledge that explains how knowledge related to cyber risk management and organizational leadership accountability is created and applied in various forms throughout organizations.

There are three major philosophical perspectives concerning epistemology. They are positivism, interpretivism and pragmatism (Collis & Hussey, 2014). Positivism emphasizes measurement using quantifiable data and statistical analysis. Interpretivism emphasizes subjectively understanding socially constructed meanings. Given the complexities surrounding cyber risk management involving both measurable organizational behaviors and human behavior, the researcher chose to use pragmatism philosophy for this study.

3.2.1 Pragmatism

Pragmatic philosophy is focused on creating practical outcomes through multiple approaches to analyze complex phenomena. The pragmatic philosophy recognizes that individuals have their own interpretations of what constitutes reality. Therefore, a singular viewpoint cannot provide an all-encompassing understanding of issues such as accountability of leadership and governance of cyber-risk (Collis & Hussey, 2014) . As a result, the pragmatic philosophy supports the use of multiple realities and quantitative/qualitative methodologies to develop a comprehensive understanding of a research problem.

This study has particular relevance because governance of cyber-risk is a complex phenomenon which encompasses technological systems, organizational processes and human decision-making. Through pragmatic philosophy, researchers are able to examine each of these aspects

from differing perspectives and synthesize meaningful conclusions. Additionally, this approach is consistent with the purpose of developing a practical and applicable framework for Zimbabwe's financial service industry to promote leadership accountability.

Additionally, Thi (2017) noted that pragmatics emphasizes shared meanings and joint actions among participants in organizations. Since leadership accountability is enacted through interactions between leaders, staff and other governance structures, the findings of this study will contribute toward the development of an understanding of how leadership accountability is implemented in practice. Finally, Hair et al. (2015) emphasized that theory can be both contextualized and generalized based upon its application and interpretation.

Adopting pragmatism allows researchers to switch between qualitative and quantitative data which are usually seen as incompatible in traditional research approaches (Thi, 2017). In this study quantitative data will measure patterns and relationships in cyber risk governance while qualitative data will probe deeper into leadership practices and dynamics of organizations. Flexibility in this way improves robustness and credibility of results. Pragmatism also lets researchers consider both influence of social actors and structural aspects of governance and this gives a balanced view (Kothari, 2019). This is especially important in Zimbabwe because realities of organizations, resource constraints and regulatory environments strongly shape governance of cyber risks.

3.3 Research Approach: Mixed Methods Approach

This study uses an integrated mixed-methods design. In this methodology both qualitative and quantitative methods are used together as part of a single study. The use of the term "mixed" refers to the combination of different forms of data through the collection, analysis, and integration of both qualitative and quantitative data so that a fuller view can be gained about a particular research question or issue (Saunders et al. 2019; Creswell & Creswell, 2018).

A justification for using an integrated mixed-methods design was because the study sought to examine both the measurable aspects of Cyber Risk Governance (CRG) and the experiences/perceptions of Leadership in Financial Institutions (FIs). A key advantage of using both quantitative and qualitative data is that it enables the researcher to identify patterns and relationships (quantitative), and to gain greater insight into leadership behaviour,

organizational culture/dynamics and CRG practice/implementation (qualitative) (Kothari, 2019).

More recently there has been increased emphasis on the advantages of conducting mixed-methods research due to its ability to enhance the validity and reliability of results through the triangulation of data across multiple datasets (Mertens, 2015; Creswell, 2018); additionally, it permits the strengths of each methodology to offset the weaknesses inherent in the use of either methodology individually, thus providing more complete and reliable results (Hair et al. 2015).

3.4 Research Design

A research design is a comprehensive outline of the methodology and strategies to be used to collect and analyze data so as to provide answers to research questions and meet the objectives of the study (Saunders, Lewis, & Thornhill, 2019). It explains how researchers can utilize different methodologies to create valid and reliable findings (Saunders et al., 2019). There are many types of research designs including experimental, survey, case study, action research, grounded theory, ethnographic and archival studies (Glaser & Strauss, 2017; Saunders et al., 2019).

This study uses a pragmatic parallel (convergent) mixed-methods design. Qualitative and quantitative data were collected at the same time. However, each set of data was analyzed individually and then combined when interpreting results. The use of a convergent design allows for an assessment of similarities/differences between the results from each data type (Creswell, 2018). Quantitative data were collected using standardized questionnaires. Semi-standardized interview schedules were used to collect qualitative data. Each set of data was analyzed separately before being combined to produce complete conclusions about leadership accountability. Convergence between the two data types increases the validity of the study findings since the results from both data types were verified against one another. The concurrent nature of the study's design makes it ideal for examining accountability within a specific organization based on both numerical and experiential evidence. This is consistent with the goal of creating a country-specific model for cyber-risk governance in Zimbabwe.

Both a survey and a case-study research design have been utilized in this research. The two designs complemented each other well given their alignment with the study's mixed-

methodology. They also provided the opportunity to address both the breadth and depth of the research issue. By combining the two designs, the researcher has been able to gather a significant amount of data while still being able to delve deeper into organizational practices and leadership interactions.

3.4.1 Survey Design

The Survey Design – The systematic collection of Quantitative Data From a Defined Population Using Structured Instruments Such As Questionnaires (Saunders et al., 2012) Is Widely Used in Research To Examine Relationships Between Variables and Generate Findings That Can Be Generalized to a Larger Population.

The survey design will be utilized to collect data from employees working at financial institutions in Zimbabwe, including executives, IT Professionals and Risk Management Personnel. The structured questionnaire will be used to collect Information about the Key Variables of Cyber Risk Governance Frameworks, Leadership Involvement, Organizational Constraints and Effective Cyber Risk Governance.

A Survey Design Was Selected for This Study Because It Allows the Researcher to Collect a Large Amount of Data in an Economical and Efficient Manner (Hair et al., 2015; Sekaran, 2013); It Also Allows Standardization So All Respondents Will Have the Same Questions Which Increases the Reliability of Responses as well as Enhance Comparability of Responses. Additionally, A Survey Design Provides More Control Over the Research Process Than Other Designs; Further, A Survey Design Facilitates Statistical Analysis of Data and Enables Researchers to Identify Patterns and Relationships Among Variables. This is Important for Testing the Study's Conceptual Framework That Examines the Influence of Accountability by Leaders on Outcomes Regarding Cyber Risk Governance.

3.4.2 Case Study Design

The Case Study Design is used to gain an in depth and Contextual understanding of Cyber Risk Governance Practices in Selected Financial Institutions. A case study is described as an Empirical Investigation of a Contemporary Phenomenon within its Real Life Context, specifically where the boundaries between the phenomenon and context are not well defined (Yin, 2016). This case study will be investigating Leadership Accountability's influence on

Cyber Risk Governance Practice in Selected Financial Institutions in Zimbabwe. Semi structured Interviews using Key Informant Sources (Senior Management; IT Professionals; Risk Officers) will be used to collect data.

A major advantage of the Case Study Design is it provides a Holistic and Detailed Understanding of Complex Organisational Phenomena (Bryman & Bell, 2015). It enables the researcher to investigate Real-Life Processes, Interactions and Decision Making Practices which can't be investigated using Quantitative Methods. Due to the nature of Cyber Risk Governance being influenced by many different aspects such as Organisational Culture, Leadership Behaviour and other contextual factors, the Case Study Design is especially suited to this area of study. Additionally, the Case Study Design complements the Survey Design, by allowing Qualitative Insights to Explain and Enrich the Quantitative Findings.

3.5 Target Population and Sampling

The target population includes all people from whom a sample is taken for a particular investigation. Creswell states (Creswell, 2018), "the target population is the total population of people that meet the specifications of interest to you." Kothari (Kothari, 2014) also describes a population as the whole group of entities within a certain geographic area or organizational environment that is being studied.

3.5.1 Population definition for this study

For this study, the target population included employees and other stakeholders that were part of a company's cyber risk governance and decision-making process. Participants consisted of senior executives, it and cybersecurity specialists, risk management personnel, compliance officers and internal auditors working for some of the largest financial institutions in the country. These individuals are considered ideal candidates for participation in the study since they have the most relevant expertise and responsibilities regarding cyber risk governance.

3.5.2 Selection of population

Participants were selected from organizational records including but not limited to employee rosters, departmental lists and governing bodies of the participating financial institutions. All data collection will occur among individuals who are currently involved with or impacted by accountability through leadership and cyber risk governance practices. The total population size will consist of the number of eligible participants across the various participating financial institutions. The defined population will provide the foundation for sampling and allow for representation of diverse perspectives on accountability through leadership and cyber risk governance within the Zimbabwean financial services industry.

3.5.3 Sample size

A sample size refers to how many participants are chosen from the target population to represent it's characteristics in a study (Sekaran, 2013; Bryman & Bell, 2015). Choosing an adequate sample size is important to assure reliability, representation and generality to the larger population.

$$n = \frac{N}{1+N_{e^2}}$$

Where:

n = sample size

N = target population (1,000)

e = level of precision or margin of error (0.10)

Sample size calculation

$$n = \frac{1000}{1+100_{(0.10)^2}} = 91$$

Therefore, n= 91

The calculated sample size is approximately 91 respondents. However, to improve reliability, account for non-responses, and ensure adequate representation across different financial institutions and roles, the sample size was rounded up to 100 participants. This sample size is considered sufficient for the study as it allows for meaningful statistical analysis while remaining manageable in terms of data collection.

3.6 Sampling Methods and Techniques

To align with the mixed methods approach adopted in this study, both probability and non-probability sampling techniques will be used. Probability sampling will be applied in the quantitative component to ensure representativeness, while non-probability sampling will be used in the qualitative component to obtain in-depth insights from key informants.

3.6.1 Systematic Random Sampling Design (Survey)

The quantitative data collection for the research used systematic random sampling. Saundersons (et.al) (2019), define systematic random sampling as a form of probability sampling where elements are taken from a sampling frame at a regular interval. Systematic random sampling provided the researcher with a means to ensure all members of the target population had an opportunity to be selected for inclusion in the sample, thus providing greater representation through the use of a representative sample.

Employees working in executive roles, IT departments, Risk Management/Compliance Departments at Financial Institutions in Zimbabwe comprised the sampling frame. Eligible participants were enumerated and assigned numbers. The sampling interval was established based on dividing the total number of individuals in the target population by the sample size. With a total population of 1,000 and a sample size of 100, every tenth person in the sampling frame would have been selected. Randomly selecting one employee from the sampling frame served as the initial selection. Subsequent selections were made systemically based on the sampling interval of ten; i.e. until the desired sample size was achieved.

Using systematic random sampling provided the researcher with a simpler way of selecting participants than other forms of sampling methods; it also offered increased efficiency when compared to some other sampling methods. In addition, systemic random sampling produced less biased selections than other sampling methods, and provided a sample that was evenly distributed throughout the population, which was critical in capturing the variation among practices of cyber risk management and leadership accountability.

3.6.2 Purposive Sampling Design (Interviews)

A purposeful sampling strategy was implemented for the qualitative element of this study. Purposeful sampling is a type of non-probability sampling. In particular, "purposeful sampling" refers to the selection of participants based on their knowledge, experience and relevance to the topic of your research (Creswell, 2014).

The purposeful sampling strategy was used for selecting knowledgeable informant who have been actively involved in Cyber Risk Governance at Financial Institutions. The participants were senior executives; IT and cybersecurity professionals; risk managers and compliance officers. Due to their specific expertise and experience they could provide insightful information with regard to Leadership Accountability as well as Governance Practices. Twenty key-informant interviews were planned. The number of interviewees was considered adequate to obtain data saturation. Data saturation occurs when no further themes are developed through additional interviews. Although purposeful sampling does not enable statistical generalization it enables the researcher to develop reliable and detailed insights about the examined cases (Bhattacherjee, 2012).

3.6.3 Questionnaires

The structured questionnaire employed for the quantitative component of the study was utilised to obtain the data required by the respondents. Questionnaires are formally defined as instruments intended to elicit direct feedback from respondents relating to their behaviour, perception, knowledge, attitude and belief towards specific topics or themes (Bryman & Bell, 2015). In addition to providing an opportunity to collect substantial amounts of data over a relatively short time frame (Bernard, 2011; Creswell, 2014), employing questionnaires in the current study allowed for uniformity in responding to the questions posed, thus facilitating the objective and scientifically based evaluation of the results obtained.

The questionnaire contained structured questions, each of which corresponded to one of the variables studied in this investigation, namely cyber risk management governance structures, leader participation, limitations imposed by organisations, developing context-specific framework and successful cyber risk management governance. Each of these questions were presented via a five point likert scale. Whereby respondents could select one of the following options: Strongly Agree = 5, Agree = 4, Neutral = 3, Disagree = 2 and Strongly Disagree = 1.

This approach was chosen due to its simplicity, ease of understanding and convenience to respondents, resulting in improved respondent rates.

A covering letter was attached to each questionnaire outlining the purpose of the study and ensuring that all information gathered would remain confidential and be utilised solely for educational purposes. Confidentiality and anonymity were maintained at all stages of the research process. Instructions were clearly stated to enable respondents to correctly complete the questionnaire.

Questionnaires were administered through self-reporting methods, e-mail and/or online platforms, thereby enabling flexible access to respondents from various financial institutions. Respondents were given approximately seven days to complete and submit their respective questionnaires. By virtue of having a well-defined structure and logical organisation to the questionnaire, respondents were able to comprehend what was being asked of them and provide correct responses.

3.6.4 Interview Guide

To obtain qualitative data for this research a structured interview guide was created to gather extensive data from those who would provide the most valuable information to support the study's objectives. Purposive sampling was used to select participants. It is essential when using purposive sampling, that individuals selected have some level of expertise/knowledge about the subject being researched (Creswell, 2018). Structured interviews were used as they represent a middle ground between open ended interviewing and closed questioning. They allow the interviewer to ask pre-determined questions while allowing them to delve further into an issue if it presents itself (Bryman & Bell, 2015). As such structured interviews are a viable method for collecting data; they enable the researcher to clarify any ambiguous questions posed during the interview and follow up to gain additional insight from the participant (Saunders, Lewis, & Thornhill, 2019).

The interview guide was developed around the study's objectives and included open ended questions related to leadership accountability, organisational governance practices and the challenges faced by organisations in terms of cyber risk management. In developing the interview guide, consideration was given to avoid asking long/vague/double barrelled

questions, and avoid leading questions to prevent biasing the participant's response. Using interviews as part of the methodology will add richness and depth to the questionnaire data collected by highlighting the specific leadership practices and organisation dynamics that can only be identified through qualitative methodologies.

3.7 Data Collection Procedure

The data collection process described how both quantitative and qualitative data were gathered using a systematic approach.

For the quantitative component of the study, questionnaire's were distributed via email, online platforms and self administration to selected respondents.

Respondents were provided sufficient time (approximately one week) to complete the questionnaire and return them.

Follow ups were conducted to improve response rates.

For the qualitative component of the study, appointments were scheduled with selected key informants who participated in interviews.

Interviews were either completed face to face or via online platform depending on participant availability and preference.

Prior to the interview participants were informed of the purpose of the study and their consent was obtained.

All ethical considerations including confidentiality and voluntary participation were adhered to throughout the data collection process.

Both structured questionnaire's and semi structured interviews ensured comprehensive data collection; this allowed the study to capture measurable trends as well as in depth insights into leadership accountability in cyber risk governance within the financial services sector in Zimbabwe.

3.8 Data Analysis

This study allowed for the analysis of both qualitative and quantitative data in an integrated manner. This approach enabled the researcher to combine numerical data with descriptive insights, thereby providing a comprehensive understanding of leadership accountability in cyber risk governance within the financial services sector in Zimbabwe.

3.8.1 Quantitative Data Analysis Techniques

The first step in quantitative data analysis was to assess the normality of the data. This is an assumption that has to be made before analyzing data statistically. Checking the normality of data will help determine if your data follows a normal distribution. Additionally, it will also help guide the selection of an appropriate statistical test (Mertler & Reinhart, 2017).

If the data was found to be normally distributed, you can conduct a parametric test. Parametric tests are many types, but some examples include: t-test for determining mean differences between two or more groups; and Pearson's r for testing the relationship between two continuous variable. If the data does not follow a normal curve, you can use a non-parametric test.Nonparametric tests can also be referred to as distribution-free tests or tests based on ranks. In this case examples of nonparametric tests included Spearman's rho for determining the relationship between continuous variables; Mann- Whitney U Test to compare medians between two independent groups; and Kruskal Wallis H Test to compare medians between three or more independent groups.

Analysis occurred in two steps. First descriptive analysis took place. Descriptive statistics summarize the demographics of participants and provide descriptions of how all participants responded. Means, standard deviations, skewness, and kurtosis measures were used to evaluate central tendencies, variability, and degree of consensus among all participants. Second, after completing the descriptive analysis, inferential analysis took place. Inferential statistics examined the association between variables, and tested each hypothesis. Correlation analysis was used to measure the strength and direction of associations between leadership accountability and effective cyber risk governance. Additionally, multiple regression analysis measured the influence of multiple independent variables on the dependent variable. Using SPSS Software supported the completion of both types of analyses, since it provided many statistical functions, including those for correlational and regression analysis.

3.8.2 Qualitative Data Analysis

Thematic Content Analysis (TCA) is a qualitative methodology that identifies, analyzes, and reports on recurring themes or patterns in data. TCA is ideal for an in-depth exploration of participant's experiences and views.

The first step in conducting TCA was to create a written transcript from each recorded interview. All interviews were transcribed verbatim to maintain as much detail as possible. To confirm the accuracy of the transcriptions, they were compared to the original recordings. Additionally, notes taken during interviews were added to the transcripts to further enhance the richness of the data.

Following the creation of the written transcripts, the data were organized around the research objectives and questions. Organizing the data involved breaking it down into discrete segments and assigning labels to those segments. Open coding, followed by axial coding provided a means for establishing relationships between the segments of data. NVivo was utilized to support and assist in organizing the data; facilitating the coding process; and identifying potential themes and sub-themes. Conducting thematic analysis enabled the systematic interpretation of the data and facilitated insight into how leaders are held accountable for cyber risk management, and what methods organizations utilize to govern cyber risks.

3.9 Validity and Reliability

Reliability is defined as the degree that a research tool or instrument produces consistent results over time when measuring a variable (Collis & Hussey, 2014) . Consistency has been demonstrated in the use of systematic methods for obtaining data from all participants (quantitative and qualitative) and the use of data collection tools. To obtain reliable quantitative data, Cronbach's Alpha coefficient was utilized to establish internal consistency among items on a scale or survey. The acceptable level for Cronbach's Alpha coefficient is considered to be > 0.70 according to Malhotra (2010), Saunders et al. (2019) and Taber (2017).

To enhance reliability for qualitative data, systematic procedures were employed including comparing information gathered consistently throughout the data collection process (constant comparison), identifying and incorporating into analysis, responses from participants that did

not fit expected categories (deviant cases); and verifying participant responses through multiple reviews and through triangulating the data (repeated review and triangulation).

3.10 Trustworthiness

Trustworthiness in this study was ensured through four key aspects. Credibility was achieved by using probing questions and triangulating interview and survey data to accurately reflect participants' views. Transferability was supported by providing detailed contextual descriptions of Zimbabwe's financial services sector, allowing findings to be applicable to similar settings. Dependability was ensured through a clear and consistent research process, including systematic data collection and analysis procedures. Confirmability was maintained by minimising researcher bias through accurate transcription, use of audit trails, and verification of findings against original data. Together, these measures enhanced the reliability and validity of the qualitative findings.

3.11 Ethical Considerations

We provided a secure and ethical study environment for all participants as well as ensured that the integrity of this study was upheld by adhering to established academic research practices regarding ethics.

Given that Cyber Risk Governance is a sensitive issue in Financial Institutions, it was very important to address ethics in our study.

Prior to collecting data, we collected informed consent from every participant. The participants were fully disclosed on the intent, scope, and validity of our research before conducting any surveys or interviews. They also signed an informed consent form indicating that they agreed to be a part of the study.

All participation in the study was by choice (i.e., "voluntary") and respondents were made aware of their rights to withdraw from participating in the data gathering process at anytime without experiencing any adverse effects. Therefore, participation was based solely upon a respondent's own desire rather than as a result of coercion.

Participants' rights to Anonymity and Confidentiality were also respected. No respondents were asked to identify themselves, and all information collected from them was treated with absolute confidentiality. The data collected were reported using Aggregated format, so no one would be able to associate a particular response with a specific respondent or institution.

Finally, we assured that all data collected in support of this study were utilized exclusively for Academic Purposes. We took full responsibility for how we handled all the information that we collected from respondents. We kept all data safely stored and secured against unauthorized access.

3.12 Chapter Summary

This chapter has presented the research methodology that was used in the study. In addition to justifying the use of a pragmatic paradigm (which combines elements of positivist and interpretivist paradigms) and using a mixed-methods approach; it described how the study would employ a parallel design (i.e., two separate studies). This chapter has covered the research strategies employed in the study (such as survey, case study etc.), and sampling techniques that could be utilised. Further details have been provided on how data will be collected (for example through questionnaires or interviews), and data analysis procedures which will be employed. Lastly issues concerning validity, reliability and ethical considerations have been examined to provide evidence of the quality of the research. A combination of both quantitative measurements and qualitative understanding of an organisation's practices is enabled by employing the mixed methods approach in this study to provide an appropriate methodological structure to assess the leadership accountability in cyber risk governance.

CHAPTER 4: DATA PRESENTATION, ANALYSIS, INTERPRETION AND DISCUSSSION

4.1 Introduction

This Chapter has been used as an opportunity to present, evaluate and interpret findings regarding Leadership Accountability within Cyber Risk Governance for Financial Services Sector in Zimbabwe. The chapter will be organized around the Research Objectives, and in addition it will attempt to address the Research Questions. This chapter will begin with an analysis of the survey response rate followed by a descriptive analysis of respondents demographic characteristics providing context to understand the subsequent quantitative data. The quantitative data collected during the study will then be analyzed using statistical methods for both descriptive statistics and inferential statistics to examine relationships among key variables including governance structures (for example internal audit function) leadership involvement organizational constraints and effective cyber risk governance. The results from the qualitative aspects of this research will also be analyzed using thematic techniques to obtain deeper insights into the data collected.

4.2 Response Rate (Analysis)

The study achieved a high response rate, which enhances the reliability and credibility of the findings. Out of the questionnaires administered, a total response rate of 97% was obtained, indicating strong participation from respondents. For the qualitative component, the interview response rate was 80%, which is also considered high and adequate for qualitative analysis.

Instrument	Administered	Responses	Unusable	Percentage
Questionnaire	**100**	97	0	97%
Interview	**20**	**16**	**0**	**80%**

Table 4-1: Response Rate

As stated by Saunders et al. (2019), if a research project achieves a response rate greater than 70%, then it may be considered an “Excellent” response rate; this would suggest that the sample in the study is likely representative and therefore appropriate for use in the data analysis

process. In addition, with a response rate greater than 70% there is less likelihood of Non-Response Bias occurring and therefore the validity of all aspects of the study will have been increased. The researcher experienced high levels of participation from the survey participants due to a number of factors including but limited to the fact that the topic areas of Leadership Accountability and Cyber Risk Governance are highly relevant to the Financial Services Sector.

4.3 DEMOGRAPHIC DATA ANALYSIS

4.3.1 Age Distribution

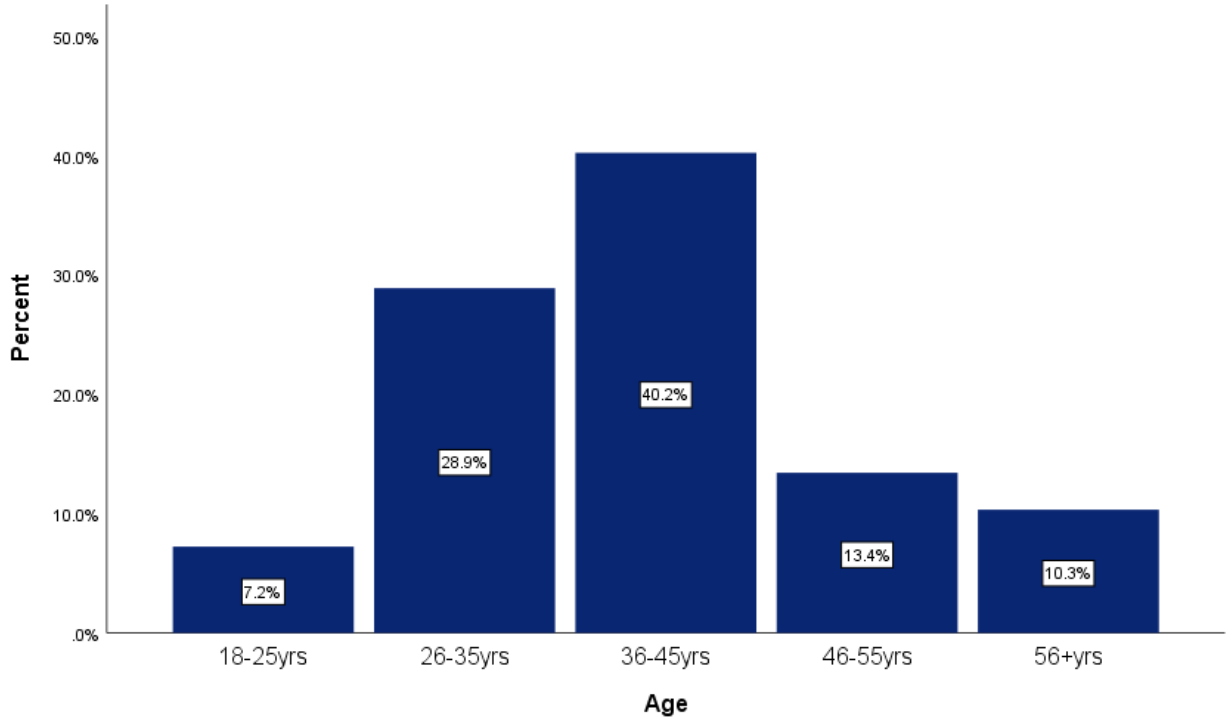


Figure 4.1:Age Distribution

The age distribution shows that the largest number of respondents fell into the "36- to 45-year-old" category (40.2%); secondly, the "26- to 35-year-old" category (28.9%) — both categories are indicative of a substantial number of people who are likely to be at a point in their careers where they have gained some experience but may still be considered to be at a relatively early stage in their careers. Thirdly, the 46- to 55-year old category comprised 13.4% of all respondents; fourthly, those aged 56 and older made up 10.3% of the sample. The 18- to 25-year old category comprised the smallest proportion of all categories, namely, 7.2%. This is

indicative of very little representation or participation of younger adults within the governance role.

4.3.2 Gender

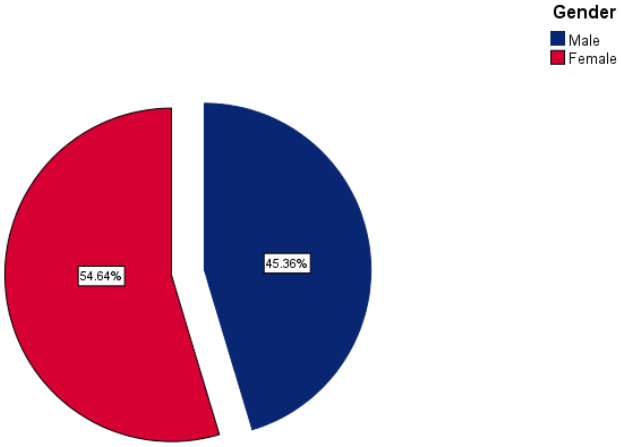


Figure 4.2: Gender

The gender distribution of respondents indicates a relatively balanced representation, with a slight majority of female respondents (54.6%) compared to male respondents (45.4%). This suggests that both genders were adequately represented in the study, allowing for diverse perspectives on leadership accountability and cyber risk governance.

4.3.3 Educational Qualification

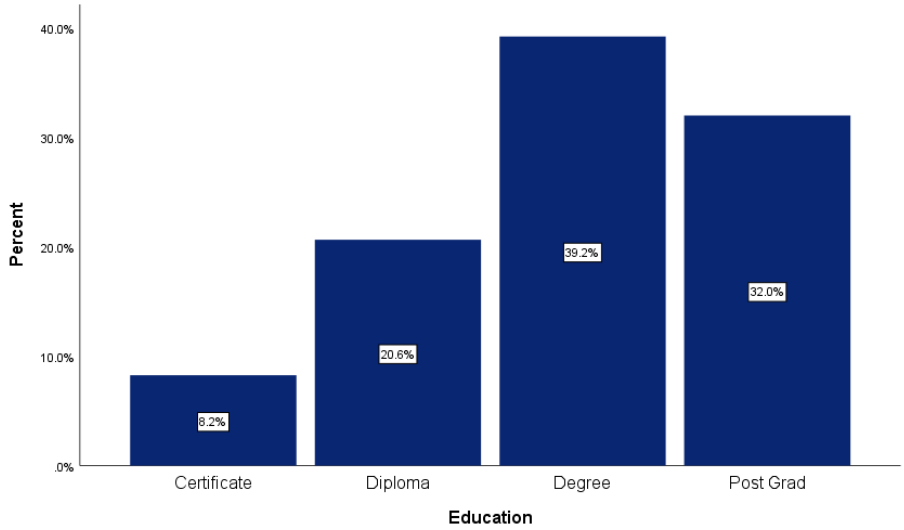


Figure 4.3: Education

Three out of four survey participants were highly educated. Nearly three out of four of them earned a college degree (39.2%) or graduate degree (32.0%). The remaining one quarter consisted of an additional 20.6 percent who earned a diploma; and 8.2 percent with a certificate (least among the four). It may therefore reasonably be assumed that at least 70 percent of all respondents are well-educated enough to understand the complexities surrounding issues like leadership accountability; and cyber risk governance. 1. I could assume that most of this group is knowledgeable and experienced in their field.

4.3.4 Position

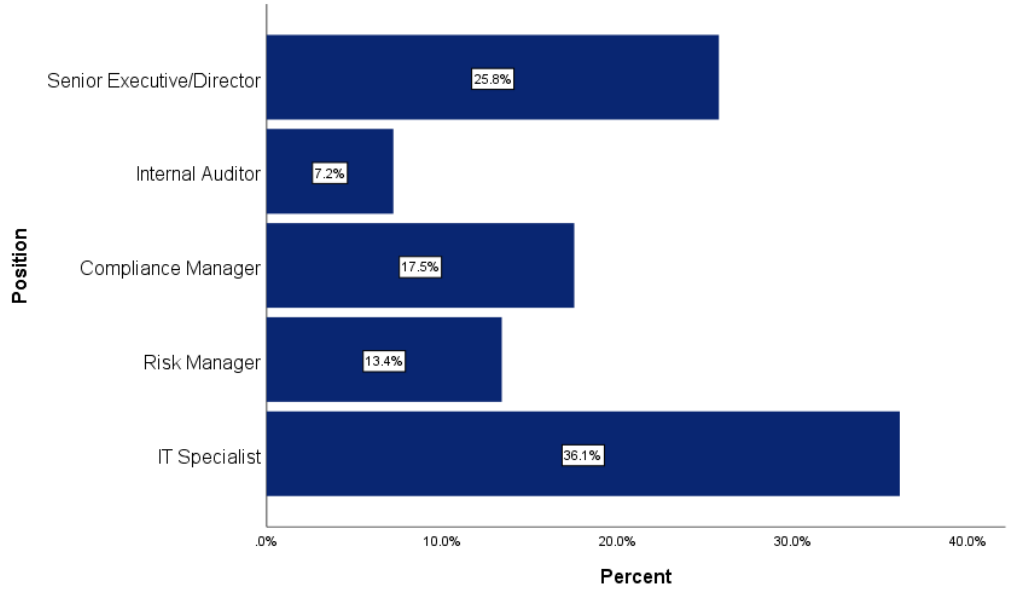


Figure 4.4: Position

The data shows that there are people in almost all job types, especially those associated with cybersecurity at banks. IT Specialist's represent the largest share of respondents (36.1%), as it is they who have the most knowledge about how to protect bank computers. The second largest number of respondents were Senior Executive/Director (25.8%); this suggests that many senior executives/directors participated; and therefore, can assess their own accountability. There were also large numbers of Compliance Manager (17.5%), Risk Manager (13.4%), and Internal Auditor (7.2%), suggesting significant participation by Governance/Oversight, Assurance/Control Mechanisms and others.

4.3.5 Type of Institution

Institution					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Bank	38	39.2	39.2	39.2
	Insurance	18	18.6	18.6	57.7
	Investment Firm	14	14.4	14.4	72.2
	Microfinance	14	14.4	14.4	86.6
	Fintech	13	13.4	13.4	100.0
	Total	97	100.0	100.0	

Table 4-2 Type of Institution

A large portion of participants (39.2%) represented banks and banking organizations. Banking organizations are typically a part of the central role within the nation's financial system and as such are at risk to cyber threats. Of the total number of participants, approximately 18.6 percent represented insurance companies. Microfinance and investment firms each comprised 14.4 percent of participants, while fintech companies were 13.4 percent of participants. Overall, it appears the distribution of participant organizations was relatively even across all of the participant organization types. Therefore, the findings from the survey can be expected to represent many different views on how accountable financial services leaders should be for cyber threat governance in Zimbabwe's financial services sector.

4.3.6 Profile of Interview Participants

Pseudonym	Gender	Age Group	Position	Type of Institution
P1	Male	36–45	IT Specialist	Bank
P2	Female	26–35	Compliance Manager	Insurance
P3	Male	46–55	Risk Manager	Bank
P4	Female	36–45	Senior Executive	Investment Firm
P5	Male	26–35	IT Specialist	Fintech
P6	Female	36–45	Risk Manager	Microfinance
P7	Male	56+	Senior Executive	Bank
P8	Female	46–55	Compliance Manager	Insurance
P9	Male	36–45	IT Specialist	Investment Firm
P10	Female	26–35	Internal Auditor	Microfinance
P11	Male	46–55	Senior Executive	Bank
P12	Female	36–45	IT Specialist	Fintech
P13	Male	26–35	Risk Manager	Insurance
P14	Female	36–45	Compliance Manager	Bank
P15	Male	46–55	IT Specialist	Fintech
P16	Female	56+	Senior Executive	Investment Firm

Table 4-3: Profile of Interview Participants

The demographics of the individuals interviewed represent an inclusive and representative sample group by a number of different means. The sample included both men and women to ensure that each gender would be equally represented. A large proportion of those who participated fall into the age category of 25-54 years old, which represents both middle-aged and older employees in their respective careers and therefore provide a combination of mid-level career development and senior level experienced employees for cyber risk governance. Those participating have been assigned to important roles such as IT specialist, Risk Manager, Compliance Manager and Senior Executive; they are able to provide both technical (from an IT standpoint) and strategic (from an organizational standpoint) insight into cyber risk governance. In addition, participation was solicited from banks, insurance companies, fintech companies, micro-finance organizations, and investment companies; this variety of sectors provides a greater degree of validity and richer data than a single sector or type of organization can provide.

4.4 Descriptive Analysis Measures

Descriptive statistical methods

Methods used in this research to describe and explain the findings from the study on areas of leadership responsibility and managing risks in cyber in the Zimbabwean Financial Services sector include quantitative methods.

Statistics on central tendency and dispersion were also calculated as well as the data trends and variations based on response data.

Example of descriptive statistics calculated for each construct (cyber risk governance frameworks, leadership involvement, organisational constraints, effective cyber risk governance)

Means were calculated to determine how much respondent's agree or disagree with each item representing the respective constructs.

When mean scores are greater than 3 ($m > 3$), it can be inferred that respondents have a general consensus regarding their perception of the constructs.

Standard deviation: was also calculated to measure the variation within the response data.

Lower standard deviations = respondents agree/converge on the response data.

Higher standard deviations = respondents disagree/diverge from the response data.

Coefficients of variance (CV): were utilized to determine how much the responses vary. $CV<1$ = small variability in responses, $CV>1$= large variability in responses.

Skewness of the data: using Skewness.

Values close to Zero are symmetrical distributions. Negative values suggest left-skewed data. Positive values represent right-skewed data

4.4.1 Analysis of Cyber Risk Governance Frameworks in the financial sector

Variable	Mean	Std. Deviation	Skewness	Std. Error (Skewness)	Kurtosis	Std. Error (Kurtosis)
Governance frameworks define roles and responsibilities	3.61	0.605	0.437	0.245	-0.639	0.485
Policies and frameworks are effectively implemented	3.41	0.933	-0.290	0.245	-0.979	0.485
Governance frameworks integrated into organisational strategy	3.75	0.736	-1.329	0.245	3.281	0.485

Table 4-4: Analysis of Cyber Risk Governance Frameworks

The study demonstrates that cyber risk governance frameworks are present in the majority of financial institutions however their success relies heavily upon the consistency in their implementation as well as the level of leadership involvement. These conclusions are consistent with studies supporting the position that cyber risk governance should not merely include technical controls but also become a part of an organization's overall strategy, decisions, and accountable processes (Mohammed Alharbi, 2025; Kikuchi & Okubo, 2019).

The average of 3.75 (SD = .736) for strategic integration corresponds with the views of Bongiovanni et al. (2024) who assert that cyber risk governance will likely be successful if included within enterprise-wide risk management and has been extended beyond the confines of the IT department. In addition, Slapničar et al. (2023) emphasize that governance models require clear lines of responsibility from top-down through middle-management, risk oversight, assurance functions, and ultimately the Board. As evidenced below, this perspective was shared by one participant:

"…the board receives regular cyber risk reporting and is directly involved in establishing the organizations' risk tolerance." (Senior Executive – P4, Investment Firm)

In addition to the previously mentioned means of ensuring accountability through clearly established role definitions (M=3.61, SD=.605); the three lines model (as emphasized by Bongiovanni et al., 2024) differentiates among those responsible for operational management, risk oversight, and independent assurance. This differentiation was also evident within one participants response:

"…our cyber risk framework follows ISO guidelines and we define roles amongst our IT, risk, and compliance teams." (Risk Manager- P3, Bank)

However, while the above-mentioned measures were demonstrated to some degree regarding accountability through role definitions, there appears to be a gap in how effectively these frameworks are implemented. The relatively low mean score for effective implementation (M=3.41, SD=0.933) supports this assertion as frameworks do not appear to be consistently implemented. Consistent with the findings of Falco et al. (2021), several participants indicated that they encounter difficulties in translating their organizational cyber governance framework into practical application based on fragmented responsibilities and lack of strategic engagement. Similar to Sharma et al. (2021) the study also indicates that cross border and digitally connected financial systems experience governance issues specifically in regards to compliance, policy implementation and technological complexities.

As seen below a similar concern was expressed during interviews:

"we have policies that exist…however enforcement can be inconsistent at times particularly at the operational level" (Internal Auditor-P10, Microfinance)

As suggested by Michael (2026), the study also indicates that continuous review and adaptation are essential for maintaining flexibility in regard to cyber threats evolving continuously. A similar perspective was expressed by a participant:

"it works, but it needs to be continually updated and trained to continue being effective." (IT Specialist-P12, Fintech)

The overall results indicate that the literature is correct in indicating that implementing effective cyber risk governance involves much more than developing and implementing frameworks. Rather than merely existing, effective cyber risk governance requires active participation from leadership, clear accountability for all individuals participating in the process, sufficient resources available for all necessary components of the process including continuous evaluation/monitoring and context specific adaptations to ensure continued viability (Slapničar et al., 2023; Maphosa, 2024; Bongiovanni et al., 2024).

4.4.2 Analysis of leadership involvement

Variable	Mean	Std. Deviation	Skewness	Std. Error (Skewness)	Kurtosis	Std. Error (Kurtosis)

Senior management participation in cyber risk decisions	2.80	1.264	-0.001	0.245	-1.002	0.485
Leadership ensures adequate cybersecurity resources	2.44	1.330	0.490	0.245	-1.028	0.485
Board reviews cyber risk governance and performance	3.02	0.901	0.482	0.245	-0.220	0.485

Table 4-5: Analysis of leadership involvement

Descriptive statistical analysis indicates a low level of participation by senior managers in the evaluation of cyber risk across all sampled financial institutions. Both the mean (M=2.80, SD=1.264) and median scores regarding the participation of senior managers in cyber risk evaluations fell well below the neutral threshold, which suggests that most survey respondents disagreed about senior manager's role in evaluating cyber risk. Likewise, both the mean (M=2.44, SD=1.33) and median scores related to the proportion of allocated resources to cybersecurity fell below the neutral threshold; therefore, respondents generally agreed that senior management has not been allocating sufficient resources toward investing in cybersecurity. On the other hand, although slightly greater than neutral, the mean (M=3.02, SD=0.90) and median scores regarding senior management review of cyber risk governance indicated a moderate level of senior manager involvement at the oversight level. The large standard deviation values for senior manager participation and resources allocated to cybersecurity indicate that many financial institutions exhibited considerable variability in their levels of senior management involvement. This suggests that some senior managers are very active in evaluating cyber risk and/or providing adequate resources toward implementing cybersecurity measures whereas others appear to be either less involved or simply uninformed regarding cyber risks. The skewness values near to zero for both items suggest that there was little bias in response patterns, and the negative kurtosis values for both items indicate that the distribution of responses were flattened.The responses indicate a variety of views about the extent to which senior management should be involved in cybersecurity decision-making. The qualitative data collected during interviews provided additional support for the quantitative results. Many interview respondents indicated that their companies' senior executives were insufficiently involved in creating corporate-wide cybersecurity policies due to limited knowledge of cybersecurity-related topics.

For example one respondent said: “Mostly, [cyber] decisions are made by IT groups and senior management doesn’t get involved unless we’ve had a big incident.” (Interviewee P1 – IT Specialist at Bank).

Other respondents noted that whether or not senior management involvement in cybersecurity decision-making leads to a focus on cybersecurity as a business-strategic issue versus a technical/operational issue depends upon the degree of engagement of senior management in decision-making regarding cybersecurity. For example: “[When] Leadership is engaged in decision-making around cybersecurity, it moves from being strictly a technology issue to becoming a strategic issue.” (Interviewee P6 – Risk Manager at Microfinance).

Many respondents noted that various organizational characteristics limited their ability to effectively manage and respond to cyber threats. They identified both structural barriers (e.g., inadequate communication among departmental units) and cultural barriers (e.g., “leadership does not take ownership of cyber risks” as per Interviewee P10 – Internal Auditor at Microfinance) as important constraints.

In addition, many respondents noted that budgetary and skills-based limitations constrained their organizations’ effectiveness in implementing meaningful cybersecurity practices. For example, as was observed by Interviewee P12 – IT Specialist at Fintech: “It’s hard to implement effective cybersecurity measures due to budgetary concerns and the lack of skilled people to do it.”

Lastly, some respondents also indicated that organizational culture could limit employees’ willingness to adhere to security policy even when those policies are very robust. As was observed by Interviewee P8 – Compliance Manager at Insurance: “If we don’t value security in our culture, then no matter how good our policies are, employees will not follow them.

Variable	Mean	Std. Deviation	Skewness	Std. Error (Skewness)	Kurtosis	Std. Error (Kurtosis)
Limited financial resources affect cyber risk governance	3.74	0.939	-0.540	0.245	-0.500	0.485
Skills shortages hinder effective governance	3.54	0.765	-0.267	0.245	0.513	0.485
Organisational culture affects accountability in cyber risk management	3.94	0.592	-1.525	0.245	6.832	0.485

Table 4-6: Analysis of Organisational Constraints

These findings align with existing literature. Bongiovanni et al. (2024) argue that many organisations struggle with limited leadership engagement, often delegating cybersecurity responsibilities to IT departments, which weakens governance effectiveness. Similarly, Falco et al. (2021) note that insufficient executive involvement leads to a disconnect between operational cybersecurity and strategic decision-making.

The low mean for resource allocation supports Sharma et al. (2021), who highlight that inadequate investment and competing organisational priorities hinder effective cyber risk management. Furthermore, Slapničar et al. (2023) emphasise that boards and executives must actively engage in cybersecurity oversight to ensure accountability and alignment with organisational goals.

The challenges related to skills and culture are consistent with Mutanda and Chrispen (2023), who identify resource constraints and varying levels of cybersecurity maturity as key barriers in developing contexts such as Zimbabwe. Additionally, Maphosa (2024) highlights that organisational culture plays a significant role in shaping cybersecurity practices and accountability.

The findings suggest that while some level of board oversight exists, leadership involvement in cybersecurity remains limited, particularly at the executive level. This weak engagement affects resource allocation, strategic prioritisation, and overall governance effectiveness, confirming the critical role of leadership accountability highlighted in the literature

The descriptive statistics indicate that organisational constraints significantly affect cyber risk governance within the financial services sector. The highest mean was recorded for organisational culture (M = 3.94, SD = 0.592), suggesting strong agreement that culture plays a critical role in shaping accountability. This was followed by limited financial resources (M = 3.74, SD = 0.939) and skills shortages (M = 3.54, SD = 0.765), indicating that both financial and human capital constraints hinder effective governance.

The relatively low standard deviation for organisational culture suggests convergence of views, while the higher variability for financial resources indicates differing experiences across institutions. The negative skewness across all variables shows that responses were concentrated towards agreement, particularly for culture (-1.525), with a high kurtosis value (6.832) indicating strong consensus.

These findings are supported by qualitative data. Participants emphasised the need for contextual adaptation:

"Cybersecurity practices have to be adjusted to our local regulatory and economic realities, especially given resource limitations" (P6, Risk Manager, Microfinance).

On improvements, respondents highlighted capacity building and investment:

"We need more investment in skills development and continuous training to keep up with evolving threats" (P12, IT Specialist, Fintech).

Regarding effectiveness, views were mixed:

"Governance structures exist, but their effectiveness is limited by budget constraints and lack of skilled personnel" (P10, Internal Auditor, Microfinance).

These findings align with literature. Mutanda and Chrispen (2023) identify resource limitations and uneven cybersecurity maturity as key challenges in Zimbabwe's financial sector. Similarly, Sharma et al. (2021) emphasise that technological complexity and limited expertise constrain governance effectiveness. The strong influence of culture supports Slapničar et al. (2023), who argue that organisational culture shapes accountability and risk behaviour. Furthermore, Ahmad and Teo (2024) highlight the importance of context-specific frameworks that reflect

local regulatory and economic conditions. Overall, the findings confirm that organisational constraints, particularly culture, resources, and skills, play a decisive role in shaping cyber risk governance effectiveness.

4.4.3 Analysis of Context-Specific Cyber Risk Governance

Variable	Mean	Std. Deviation	Skewness	Std. Error (Skewness)	Kurtosis	Std. Error (Kurtosis)
Cybersecurity strategies adapted to Zimbabwean context	3.68	0.700	-0.021	0.245	-0.227	0.485
Frameworks updated for emerging threats	3.55	0.791	0.747	0.245	-0.578	0.485
Governance aligned to regulatory and environmental conditions	3.97	0.567	-1.754	0.245	8.789	0.485

Table 4-7: Analysis of Context-Specific Cyber Risk Governance

The descriptive statistics indicate a generally positive orientation towards context-specific cyber risk governance within Zimbabwe's financial services sector. The highest mean was recorded for consideration of regulatory and environmental conditions (M = 3.97, SD = 0.567), suggesting strong agreement that institutions align governance practices with local requirements. This is followed by adaptation of cybersecurity strategies to the Zimbabwean context (M = 3.68, SD = 0.700) and continuous updating of governance frameworks (M = 3.55, SD = 0.791), indicating moderate agreement.

The low standard deviation for regulatory alignment reflects strong consensus among respondents, further supported by the high kurtosis value (8.789), indicating a concentrated distribution of agreement. The negative skewness (-1.754) also confirms that most responses leaned towards agreement. However, the slightly higher variability in framework updates suggests uneven responsiveness to emerging threats across institutions.

Qualitative findings reinforce these results. Participants emphasised the importance of contextual adaptation and leadership support:

"Strong governance comes from aligning cybersecurity strategies with local regulations and continuously adapting to new threats" (P4, Senior Executive, Investment Firm).

Another participant highlighted the role of resources and skills:

"Investment in skills and technology is key, but leadership must prioritise and drive these initiatives" (P12, IT Specialist, Fintech).

On leadership accountability, participants were explicit:

"Leadership accountability is critical because without it, cybersecurity remains an IT issue rather than a strategic priority" (P6, Risk Manager, Microfinance).

Similarly P3 stated that

"Boards need to take ownership of cyber risk and ensure that governance frameworks are not just policies but actively enforced" (P3, Risk Manager, Bank).

These findings are consistent with the literature where Ahmad and Teo (2024) emphasise that effective cyber risk governance requires context-specific adaptation to regulatory and environmental conditions. Bongiovanni et al. (2024) and Slapničar et al. (2023) argue that leadership accountability is essential in integrating cybersecurity into organisational strategy and ensuring continuous oversight. Furthermore, Falco et al. (2021) highlight the need for adaptive governance frameworks that evolve with emerging cyber threats.

The results suggest that while financial institutions in Zimbabwe recognise the importance of contextualised governance, the effectiveness of these efforts is significantly influenced by leadership accountability, continuous adaptation, and investment in resources and capabilities.

4.5 Inferential Analysis

4.5.1 Variable Definition

A definition of the variables used in this study is presented in the table below, aligned with the conceptual framework on leadership accountability and cyber risk governance in the financial services sector in Zimbabwe.

Variable	Definition
ECG (DV)	Dependent variable measuring Effective Cyber Risk Governance in financial institutions, based on responses related to risk identification, response, and governance effectiveness.
α	Constant term representing the value of the dependent variable when all independent variables are equal to zero.
β_1–β_4	Regression coefficients measuring the partial effect of each independent variable on Effective Cyber Risk Governance.
CRG (IV_1)	Independent variable measuring Cyber Risk Governance Frameworks, including structure, policies, and integration into organisational strategy.
LED (IV_2)	Independent variable measuring Leadership Involvement, including senior management participation, resource allocation, and board oversight in cybersecurity.
OCN (IV_3)	Independent variable measuring Organisational Constraints, including financial resources, skills shortages, and organisational culture affecting cyber risk governance.
FRM (IV_4)	Independent variable measuring Context-Specific Framework Development, including adaptation of cybersecurity strategies to the Zimbabwean regulatory and operational environment.
ε	Error term capturing the effect of other variables not included in the model that may influence Effective Cyber Risk Governance.

Table 4-8: 4Variable Definition

This operationalisation of variables supports the empirical analysis of how leadership accountability influences cyber risk governance outcomes in the financial services sector.

4.5.2 Reliability Testing

Reliability testing was conducted to evaluate the internal consistency of the survey instrument used to measure constructs related to leadership accountability and cyber risk governance in the financial services sector in Zimbabwe. The purpose was to ensure that the instrument consistently measured the intended variables, including cyber risk governance frameworks,

leadership involvement, organisational constraints, context-specific framework development, and effective cyber risk governance.

Cronbach's alpha coefficient was used as the measure of internal consistency. It is widely recognised as a reliable indicator, with a minimum acceptable threshold of 0.60 (Heal & Twycross, 2012; Shuttleworth, 2015).

The results from SPSS are presented below:

4.5.3 Reliability Statistics

Cronbach's Alpha	N of Items
0.780	15

Table 4-9: Reliability

The results indicate that the survey instrument achieved an overall Cronbach's alpha of 0.78 across 15 items. This value exceeds the acceptable threshold, suggesting a good level of internal consistency (Taber, 2017). Therefore, the instrument was considered reliable and suitable for further statistical analysis, as it consistently captured the constructs related to leadership accountability and cyber risk governance.

4.6 Regression Analysis

4.6.1 Model Summary

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.758[a]	.574	.556	.47866
a. Predictors: (Constant), FRM, OCN, LED, CRG				

Table 4-10: Regression Model Summary

The model summary results indicate a strong relationship between the independent variables and the dependent variable, Effective Cyber Risk Governance (ECG). The correlation coefficient (R = 0.758) suggests a strong positive association between cyber risk governance

frameworks (CRG), leadership involvement (LED), organisational constraints (OCN), and context-specific framework development (FRM) with ECG.

The R Square value of 0.574 indicates that approximately 57.4% of the variation in effective cyber risk governance is explained by the four independent variables included in the model. This demonstrates a substantial explanatory power, suggesting that leadership accountability factors play a significant role in shaping cyber risk governance outcomes. The Adjusted R Square of 0.556 shows a slight reduction, accounting for the number of predictors in the model, but still confirms a strong model fit. This implies that the model is reliable and not overly inflated by the inclusion of multiple variables.

The standard error of the estimate (0.47866) indicates a relatively low level of prediction error, suggesting that the model provides a good fit to the observed data. Overall, the results confirm that leadership accountability, as operationalised through CRG, LED, OCN, and FRM, significantly contributes to effective cyber risk governance in Zimbabwe's financial services sector

4.6.2 Anova

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	28.420	4	7.105	31.010	.000[b]
	Residual	21.079	92	.229		
	Total	49.498	96			

a. Dependent Variable: ECG

b. Predictors: (Constant), FRM, OCN, LED, CRG

Table 4-11: Anova Analysis

The ANOVA results assess the overall significance of the regression model examining the influence of CRG, LED, OCN, and FRM on Effective Cyber Risk Governance (ECG).

The findings show that the model is statistically significant ($F = 31.010$, $p = 0.000$). Since the significance value is less than 0.05, this indicates that the model provides a good fit and that the independent variables collectively have a significant effect on ECG. In other words, at least

one of the predictors meaningfully contributes to explaining variations in cyber risk governance effectiveness. The regression sum of squares (28.420) compared to the residual sum of squares (21.079) further indicates that a substantial proportion of variance in ECG is explained by the model.

4.6.3 Coefficients

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-.488	.452		-1.079	.283
	CRG	.203	.127	.153	1.597	.014
	LED	.196	.059	.290	3.302	.001
	OCN	.500	.097	.389	5.127	.000
	FRM	.247	.142	.173	1.739	.000
a. Dependent Variable: ECG						

Table 4-12: Regression Coefficients

The regression results indicate the individual contribution of each independent variable to Effective Cyber Risk Governance (ECG).

The results show β_1 (CRG) = 0.153, p = 0.014 < 0.05, t = 1.597 > 0.00, which implies that a one standard unit increase in Cyber Risk Governance Frameworks predicts an increase of 0.153 in ECG, ceteris paribus. This indicates a positive and statistically significant relationship.

For leadership involvement, the results show β_2 (LED) = 0.290, p = 0.001 < 0.05, t = 3.302 > 0.00, implying that a one standard unit increase in Leadership Involvement leads to a 0.290 increase in ECG, ceteris paribus. This demonstrates a strong and significant influence.

The results further show β_3 (OCN) = 0.389, p = 0.000 < 0.05, t = 5.127 > 0.00, indicating that Organisational Constraints have the strongest effect, where a one unit increase predicts a 0.389 increase in ECG.

Finally, β_4 (FRM) = 0.173, p = 0.000 < 0.05, t = 1.739 > 0.00 shows that Context-Specific Framework Development positively predicts ECG by 0.173.

All variables are statistically significant, with organisational constraints and leadership involvement exerting the strongest influence on effective cyber risk governance.

4.7 Application of the Findings to Education 5.0: A Heritage-Based Approach

The findings of this study have practical significance when interpreted within Zimbabwe's Education 5.0 heritage-based philosophy, particularly its emphasis on using research and innovation to address locally experienced socioeconomic and institutional problems. Rather than treating knowledge production as an end in itself, the study translates empirical evidence on leadership accountability and cyber risk governance into a context-responsive solution for Zimbabwe's financial services sector. The application of Education 5.0 is therefore reflected through problem-solving, localisation, knowledge creation, innovation and the development of a practical governance framework.

First, the findings demonstrate a clear problem-solving orientation. Although respondents indicated that cyber risk governance frameworks generally exist and are integrated into organisational strategy (M=3.75, SD=0.736), their implementation remains uneven (M=3.41, SD=0.933). More importantly, senior management participation in cyber risk decisions was relatively weak (M=2.80, SD=1.264), while leadership commitment to adequate cybersecurity resources recorded an even lower mean (M=2.44, SD=1.330). These findings identify a practical governance problem: financial institutions may possess cybersecurity policies and technical structures without corresponding leadership ownership and accountability. Consistent with Education 5.0, the study does not end with identifying this weakness. The findings provide the empirical foundation for developing a Cyber Risk Governance and Leadership Accountability Framework that can strengthen institutional responsibility for cybersecurity.

Second, the findings advance localisation and heritage-based knowledge production. The study found strong agreement that cyber risk governance should reflect Zimbabwe's regulatory and environmental conditions (M=3.97, SD=0.567), while respondents also supported adapting cybersecurity strategies specifically to the Zimbabwean context (M=3.68, SD=0.700). These findings are important because international cybersecurity standards cannot necessarily be transferred into Zimbabwean institutions without considering local regulatory structures, financial constraints, skills shortages, organisational cultures and technological conditions. This supports Ahmad and Teo's (2024) argument for context-sensitive governance frameworks. From an Education 5.0 perspective, therefore, heritage does not imply rejecting international cybersecurity standards; rather, it requires adapting global knowledge to Zimbabwe's institutional realities and locally available capabilities.

Third, the findings contribute to innovation and knowledge creation. Regression analysis established that cyber risk governance frameworks, leadership involvement, organisational constraints and context-specific framework development collectively explain 57.4% of the variation in effective cyber risk governance (R^2=0.574). Leadership involvement (β=0.290) and organisational constraints (β=0.389) emerged as particularly influential dimensions. These results shift the study beyond the assumption that cybersecurity effectiveness is principally determined by technological controls. Instead, they demonstrate that governance effectiveness is also shaped by leadership behaviour, institutional culture, resources, skills and accountability structures. This provides locally generated knowledge that can inform how Zimbabwean financial institutions conceptualise cyber resilience.

Fourth, Education 5.0's emphasis on producing tangible outputs from research is addressed through the proposed Five Lines of Accountability Framework. The framework translates the findings into clearly differentiated levels of cyber risk responsibility, moving cybersecurity from an IT-centred function towards shared institutional accountability. Drawing upon the accountability principles identified by Slapničar et al. (2023), the framework can clarify responsibility across operational management, cybersecurity and technology functions, risk and compliance structures, executive leadership, and board-level oversight. Its purpose is

therefore not merely conceptual. Financial institutions could use it to allocate cyber responsibilities, establish reporting and escalation mechanisms, assess leadership performance and determine where accountability resides when cyber governance failures occur.

The findings also create opportunities for a second practical Education 5.0 output: leadership capacity development. Skills shortages were identified as an important organisational constraint (M=3.54, SD=0.765), while participants reported limitations in leadership knowledge and cybersecurity expertise. These findings provide a basis for developing targeted executive and board training covering cyber risk literacy, governance responsibilities, incident accountability, regulatory obligations and strategic resource allocation. Training would therefore address an empirically identified institutional need rather than functioning as a generic cybersecurity intervention.

Finally, the findings can inform policy and regulatory reform. Regulators and financial institutions may use the proposed framework to reconsider whether existing governance arrangements sufficiently define board and executive accountability for cyber risk. The strong support for regulatory and environmental alignment suggests that cybersecurity governance in Zimbabwe requires mechanisms that combine international standards with domestic regulatory, economic and institutional realities. In this respect, the study gives practical expression to Education 5.0 by moving through a clear pathway from local problem identification, to empirical knowledge generation, to contextual innovation, and ultimately to an applicable governance product.

The study therefore contributes more than an assessment of cybersecurity practices. Its Education 5.0 contribution lies in converting evidence generated from Zimbabwe's financial services environment into a locally responsive Cyber Risk Governance and Leadership Accountability Framework, associated policy recommendations and a basis for leadership development. In this way, heritage-based research becomes a mechanism for strengthening

institutional capability, cyber resilience and the security of Zimbabwe's increasingly digital financial system.

4.8 Chapter Summary

This chapter presented, analysed, and interpreted the findings on leadership accountability in cyber risk governance within Zimbabwe's financial services sector. The results showed high response rates, ensuring reliability of the data. Descriptive analysis revealed that respondents were experienced and well-positioned to provide relevant insights. The findings indicated that cyber risk governance frameworks are generally in place and strategically aligned, but their implementation varies across institutions. Leadership involvement was found to be limited, particularly in resource allocation and decision-making, while organisational constraints such as culture, skills shortages, and financial limitations significantly affect governance effectiveness. Regression analysis confirmed that all independent variables significantly influence effective cyber risk governance, with organisational constraints and leadership involvement having the strongest impact.

.

CHAPTER 5: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents the concluding section of the study on leadership accountability in cyber risk governance within the financial services sector in Zimbabwe. It synthesises the key findings from the previous chapters and provides a comprehensive summary of the study. The chapter draws on the empirical results and discussions to develop well-informed conclusions regarding the role of leadership accountability in strengthening cyber risk governance. Furthermore, the chapter provides practical recommendations aimed at improving governance practices within financial institutions. It also presents a proposed context-specific leadership accountability framework designed to enhance cyber risk governance effectiveness in Zimbabwe. Finally, the chapter identifies areas for further research, highlighting gaps that require additional investigation. Overall, this chapter integrates the study findings to offer both theoretical insights and practical solutions for improving cyber risk governance.

5.2 Summary of Findings

This study investigated leadership accountability in cyber risk governance within the financial services sector in Zimbabwe. The study was guided by four key objectives: to analyse existing cyber risk governance frameworks, evaluate leadership involvement, examine organisational constraints, and develop a context-specific framework to strengthen governance effectiveness. Using a mixed methods approach, data were collected through questionnaires and interviews from financial sector professionals selected through systematic and purposive sampling. The findings revealed that cyber risk governance frameworks are generally in place and aligned with organisational strategy, although their implementation remains inconsistent across institutions.

Secondly, the study found that leadership involvement is limited, particularly in resource allocation and active participation in cyber risk decision-making. While some board-level oversight exists, cybersecurity is often treated as a technical issue rather than a strategic priority. Thirdly, the study established that organisational constraints, including limited financial resources, skills shortages, and organisational culture, significantly affect the effectiveness of cyber risk governance. These factors were found to be critical barriers to achieving strong accountability. Finally, the study confirmed that context-specific framework development, including adaptation to local regulatory and environmental conditions, plays a

significant role in enhancing governance effectiveness. Regression analysis showed that all independent variables significantly influence effective cyber risk governance, with organisational constraints and leadership involvement exerting the strongest impact.

5.3 Conclusions

Based on the statistical and thematic findings, the study draws several key conclusions regarding leadership accountability and cyber risk governance in the financial services sector in Zimbabwe.

Firstly, the study concludes that cyber risk governance frameworks have a positive and significant influence on effective cyber risk governance. Financial institutions have established governance structures that define roles and integrate cybersecurity into organisational strategy. However, the effectiveness of these frameworks is dependent on consistent implementation. This supports existing literature which emphasises that governance structures must be embedded within organisational processes to enhance risk management effectiveness (Bongiovanni et al., 2024; Kikuchi & Okubo, 2019).

Secondly, the study concludes that leadership involvement is a critical determinant of effective cyber risk governance, yet it remains insufficient in many institutions. While some board-level oversight exists, senior management participation in decision-making and resource allocation is limited. This finding reinforces the argument that cybersecurity must be driven at the strategic level rather than being confined to technical functions (Slapničar et al., 2023; Falco et al., 2021).

Thirdly, the study concludes that organisational constraints significantly affect cyber risk governance outcomes. Factors such as limited financial resources, shortage of skilled cybersecurity professionals, and weak organisational culture hinder the effective implementation of governance frameworks. This aligns with studies highlighting the challenges faced by developing economies in building cybersecurity capacity and institutional maturity (Mutanda & Chrispen, 2023; Sharma et al., 2021).

Finally, the study concludes that context-specific adaptation of cyber risk governance frameworks enhances their effectiveness. Financial institutions that align cybersecurity strategies with local regulatory and environmental conditions are better positioned to manage

cyber risks. Leadership accountability plays a central role in driving this adaptation and ensuring continuous improvement.

5.4 Recommendations

Based on the findings and conclusions of the study, the following recommendations are proposed to enhance leadership accountability in cyber risk governance within the financial services sector in Zimbabwe:

- Strengthen Executive and Board-Level Involvement

Financial institutions should ensure active participation of senior management and boards in cyber risk governance. This includes regular review of cybersecurity performance, setting risk appetite, and integrating cyber risk into strategic decision-making processes.

- Enhance Resource Allocation for Cybersecurity

Organisations should prioritise adequate financial and technological investment in cybersecurity. This includes funding for advanced security systems, continuous monitoring tools, and capacity-building initiatives to improve governance effectiveness.

- Develop Cybersecurity Skills and Training Programmes

Institutions should invest in continuous training and development of employees, particularly in cybersecurity and risk management. This will address skills shortages and improve the organisation's ability to respond to evolving cyber threats.

- Promote a Strong Cybersecurity Culture

Organisations should foster a culture of accountability and security awareness across all levels. This can be achieved through awareness programmes, clear communication of policies, and enforcement of cybersecurity practices.

- Adopt Context-Specific and Adaptive Governance Frameworks

Financial institutions should continuously update and adapt their cyber risk governance frameworks to align with Zimbabwe's regulatory environment and emerging cyber threats.

Leadership should ensure that these frameworks are not only developed but effectively implemented and monitored.

5.5 Proposed Framework

The proposed framework conceptualises cyber risk governance as a multi-layered system driven by leadership accountability within financial institutions. It extends the traditional Three Lines of Defense model into a Five Lines of Accountability approach, incorporating operational management, risk and compliance functions, internal audit, executive management, and the board of directors. Each layer plays a distinct but interconnected role in managing cyber risk, from implementing technical controls to providing strategic oversight.



Figure 5.1: Proposed Framework

At the core of the framework is leadership accountability, which acts as a critical link between governance structures and effective cyber risk outcomes. While operational and control functions provide the foundation for cybersecurity, the framework emphasises that executive management and boards are responsible for integrating cyber risk into organisational strategy,

allocating resources, and ensuring oversight. This reduces governance gaps and enhances coordination across the institution.

The framework also recognises that increasing digitalisation, system complexity, and human factors heighten cyber risk exposure. Therefore, effective governance requires a holistic approach that combines technical measures with strong leadership and organisational culture. Evidence suggests that leadership attributes such as ethical conduct and strategic foresight significantly influence risk management effectiveness

5.6 Areas for Further Study

The following are suggested areas for further studies

- Examine how leadership accountability in cyber risk governance differs between developed and developing countries to improve generalisability of findings.
- Investigate how technologies such as artificial intelligence, blockchain, and cloud computing influence cyber risk governance and leadership decision-making.
- Explore how organisational culture, leadership styles, and ethical practices affect leadership accountability and cybersecurity outcomes.

REFERENCES

Ahmad, S. A., & Teo, P. C. (2024). The implementation of enterprise risk management (ERM) frameworks in small and medium enterprises (SMES): A literature review. *International Journal of Academic Research in Business and Social Sciences*, *14*(9), 290-307.

Alam, M. K., 2021. A systematic qualitative case study: questions, data collection, NVivo analysis and saturation. Qualitative Research in Organizations and Management:. An International Journal, , 16(1), pp. 1-31..

Al-Faryan, M. A. S. (2024). Agency theory, corporate governance and corruption: an integrative literature review approach. *Cogent social sciences*, *10*(1), 2337893.

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences*, *11*(8), 3383.

Allsop, D. et al., 2022. Qualitative methods with Nvivo software: A practical guide for analyzing qualitative data.. Psych, , 4(2), pp. 142-159..

Ambore,S., Richardson, C., Dogan, S., Apeh, E and Osselton,A., (2017) A resilient cybersecurity framework for Mobile Financial Services (MFS), Journal of Cyber Security Technology, 1:3-4, 202-224,

Anton, S. G., & Nucu, A. E. A. (2020). Enterprise risk management: A literature review and agenda for future research. *Journal of Risk and Financial Management*, *13*(11), 281.

Appelbaum, S. H. (1997). Socio-technical systems theory: an intervention strategy for organizational development. *Management decision*, *35*(6), 452-463.

Auffret, J. P., Snowdon, J. L., Stavrou, A., Katz, J. S., Kelley, D., Rahman, R. S., ... & Warweg, P. (2017). Cybersecurity leadership: Competencies, governance, and technologies for industrial control systems. *Journal of Interconnection Networks*, *17*(01), 1740001.

Bhattacherjee, A., 2012. Social Science Research: Principles, Methods, and Practices. Textbooks Collection. Book 3.. Chicago: Sage.

Bongiovanni, I., Slapničar, S., Axelsen, M., & Stockdale, D. (2024). The Three Lines Model in Cybersecurity Governance and Risk Management. *ISACA Journal*, *1*.

Braun, V. & Clarke, V., 2021. To saturate or not to saturate? Questioning data saturation as a useful concept for thematic analysis and sample-size rationales.. Qualitative research in sport, exercise and health,, 13(2), pp. 201-216.

Bryman & Bell, E., 2015. Business Research Methods" 4th edition. s.l.:Oxford University Press.

Burns & Burns, 2012. Business Research Methods Using SPSS. Singapore: Sage Publications Asia-Pacific Pvt Ltd.

Chamboko, R. (2022). On the role of gender and age in the use of digital financial services in Zimbabwe. *International Journal of Financial Studies*, *10*(3), 82.

Chundu, B., Masamha, T., & Sifile, O. (2025). Cyber-security governance framework pillars for Zimbabwean local authorities. *Cogent Social Sciences*, *11*(1), 2453094.

Ciriello, R. F., Richter, A., & Mathiassen, L. (2024). Emergence of creativity in IS development teams: A socio-technical systems perspective. *International Journal of Information Management*, *74*, 102698.

Cole, C. D., & Schneider, R. (2020). Corporate governance and capital structure: Extending agency theory from executives to the board of directors. *Journal of Accounting and Finance*, *20*(6), 108-124.

Collis, J. & Hussey, R., 2014. "Business Research: A Practical Guide for Undergraduate and Postgraduate Students" 4th edition,. London: Palgrave Macmillan,.

Creswell, J. & Creswell, J. D., 2018. Research design: Qualitative, quantitative, and mixed methods approaches.. Thousand Oaks, California: Sage publications.

Creswell, J. W. & Poth, C. N., 2018. Qualitative inquiry and research design. 4th ed. Thousand Oaks, CA: Sage..

Creswell, J. W., 2014. Research Design - Qualitative, Quantitative and Mixed Methods Approaches. 5TH ed. California: Sage.

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713.

Edwards-Jones, A., 2014. Qualitative data analysis with NVIVO,. Journal of Education for Teaching, , 40(2), pp. 193-195.

Falco, G., Cornish, P., Creese, S., Carr, M., Cavelty, M. D., Eckert, C., ... & Parthasarathi, A. (2021). Cyber crossroads: A global research collaborative on cyber risk governance. *arXiv preprint arXiv:2107.14065*.

Falco, G., Cornish, P., Creese, S., Carr, M., Cavelty, M. D., Eckert, C., ... & Parthasarathi, A. (2021). Cyber crossroads: A global research collaborative on cyber risk governance. *arXiv preprint arXiv:2107.14065*.

Foya, D., & Changunda, G. (2019). An Investigation of Corporate Governance Challenges Facing Indigenous Banks in Zimbabwe. *International Journal of Research and Innovation in Social Science*, *3*(10), 100-115.the

Herrera Luque, F. J., Munera López, J., & Williams, P. (2021). Cyber risk as a threat to financial stability. *Revista de Estabilidad Financiera/Banco de España, 40 (primavera 2021), p. 181-205*.

Kikuchi, M., & Okubo, T. (2019, June). Cyber governance complex in firms. In *Proceedings of the 2nd International Conference on Control and Computer Vision* (pp. 116-120).

Madziwa, C., & Sibanda, V. (2018). An analysis of the impact of social media in the financial services sector in Zimbabwe: a customer perspective. *International Journal of Economics, Commerce and Management*, *6*(2), 248-272.

Manungo, G., Mpahlo, R., Ndhlovu, F., & Chirisa, I. (2022). Structure, Function and Performance of the Financial Services Sector in Zimbabwe since. *MANAGING EDITOR*.

Maphosa, V. (2024). An overview of cybersecurity in Zimbabwe's financial services sector. *F1000Research*, *12*, 1251.

Maphosa, V. (2024). An overview of cybersecurity in Zimbabwe's financial services sector. *F1000Research*, *12*, 1251.

Mohammed Alharbi, T. S. (2025). Cybersecurity governance and organizational resilience: A framework for sustainable risk management. *EDPACS*, 1-16.

Mugari, I., Gona, S., Maunga, M., & Chiyambiro, R. (2018). Cybercrime-the emerging threat to the financial services sector in Zimbabwe. *Mediterranean Journal of Social Sciences*, *7*(3), 135-143.

Mupokosera II, J., Mphahlele, M., Jordaan, A., & Jokonya, O. (2024, November). Information Security Culture: The Effect of Strategy, Technology, Organization, People and the Environment. In *2024 3rd Zimbabwe Conference of Information and Communication Technologies (ZCICT)* (pp. 1-7). IEEE.

Mupokosera, J. (2023, November). Financial Services Information Security Culture: The Effect of Technology, People and Environment. In *2023 2nd Zimbabwe Conference of Information and Communication Technologies (ZCICT)* (pp. 1-5). IEEE.

Mutanda, B., & Chrispen, M. (2023). Towards a cyber resilient banking system: Effectiveness of cyber fraud risk management strategies adopted by commercial banks in Zimbabwe. *Article in Studies and Scientific Researches Economics Edition*, *37*, 54-69.

Panda, B., & Leepsa, N. M. (2017). Agency theory: Review of theory and evidence on problems and perspectives. *Indian journal of corporate governance*, *10*(1), 74-95.

Peihani, M. (2022). Regulation of cyber risk in the banking system: a Canadian case study. *Journal of Financial Regulation*, *8*(2), 139-161.

Saunders, M. N. K., Lewis, P. & Thornhill, A., 2019. Research Methods for Business Student. 8th ed. Harlow, England: Pearson Education.

Sekaran, U., 2013. Research Methods for Business: A Skill-Building Approach. 6th Edition,. New York.: Wiley, .

Sharma, A., Adekunle, B. I., Ogeawuchi, J. C., Abayomi, A. A., & Onifade, O. (2021). Governance challenges in cross-border fintech operations: Policy, compliance, and cyber risk management in the digital age. *IRE Journals*, *4*(9), 1-8.

Slapničar, S., Axelsen, M., Bongiovanni, I., & Stockdale, D. (2023). A pathway model to five lines of accountability in cybersecurity governance. *International journal of accounting information systems*, *51*, 100642.

Thomas, A. (2024). Digitally transforming the organization through knowledge management: a socio-technical system (STS) perspective. *European Journal of Innovation Management*, *27*(9), 437-460.

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & security*, *88*, 101640.

Yurtseven, M. K., & Buchanan, W. W. (2013, March). Socio-technical system design: a general systems theory perspective. In *Proceedings of the International Conference on Engineering and Computer Education, ICECE*.

APPENDIX 1: QUESTIONNAIRE

My name is Clemence Chikombingo and I am a postgraduate student at Bindura University of Science Education carrying out a survey entitled ***Towards Leadership Accountability on Cyber Risk Governance in The Financial Services Sector in Zimbabwe in*** partial fulfilment of the Master of Business Leadership. You have been selected to participate in this survey because of your position in the financial sector in Harare, Zimbabwe. The survey will take a few minutes. Please note that your responses will be used solely for academic purposes.

SECTION A: DEMOGRAPHIC INFORMATION (TICK WHERE APPROPRIATE)

1. Age:		**2: Years in Fin Sector**		**3.Qualification**		**4: Gender**		**5: Position**	
+Below 25 Years		1-5 years		Diploma		Male		IT Specialist	
26-35 years		6-10 years		Degree		Female		Internal Auditor	
36-45 years		11-15 years		Masters				Compliance Manager	
46-55 years		16+ years		PhD				Risk Manager	
56+ years								Senior Executive	

SECTION B

Kindly indicate the extent to which you agree with the following statements, by ticking the appropriate box, where;

1=Strongly Disagree (SD), 2=Disagree (D), 3=Neutral (N), 4=Agree (A) and 5=Strongly Agree (SA).

No.	**Construct**	**Rating**				
A	**Cyber Risk Governance Frameworks**	1	2	3	4	5
1	Cyber risk governance frameworks in my organisation clearly define roles and responsibilities for managing cyber risk.					
2	Existing cybersecurity policies and frameworks are effectively implemented within the organisation.					

3	Cyber risk governance frameworks are integrated into overall organisational strategy.					
B	**Leadership Involvement**	1	2	3	4	5
4	Senior management actively participates in cyber risk management decisions.					
5	Leadership ensures adequate resources are allocated to cybersecurity initiatives.					
6	The board of directors regularly reviews cyber risk governance and performance.					
C	**Organisational Constraints**	1	2	3	4	5
7	Limited financial resources affect the effectiveness of cyber risk governance in my organisation.					
8	Skills shortages and lack of cybersecurity expertise hinder effective governance.					
9	Organisational culture affects the level of accountability in managing cyber risks.					
D	**Context-Specific Framework Development**	1	2	3	4	5
10	Cybersecurity strategies in my organisation are adapted to the local Zimbabwean context.					
11	The organisation continuously updates its cyber risk governance framework to respond to emerging threats.					
12	Cyber risk governance practices consider regulatory and environmental conditions specific to Zimbabwe.					
E	**Effective Cyber Risk Governance**	1	2	3	4	5
13	My organisation effectively identifies and assesses cyber risks.					
14	The organisation responds proactively to cybersecurity threats and incidents.					
15	Cyber risk governance in my organisation enhances overall organisational resilience and compliance.					

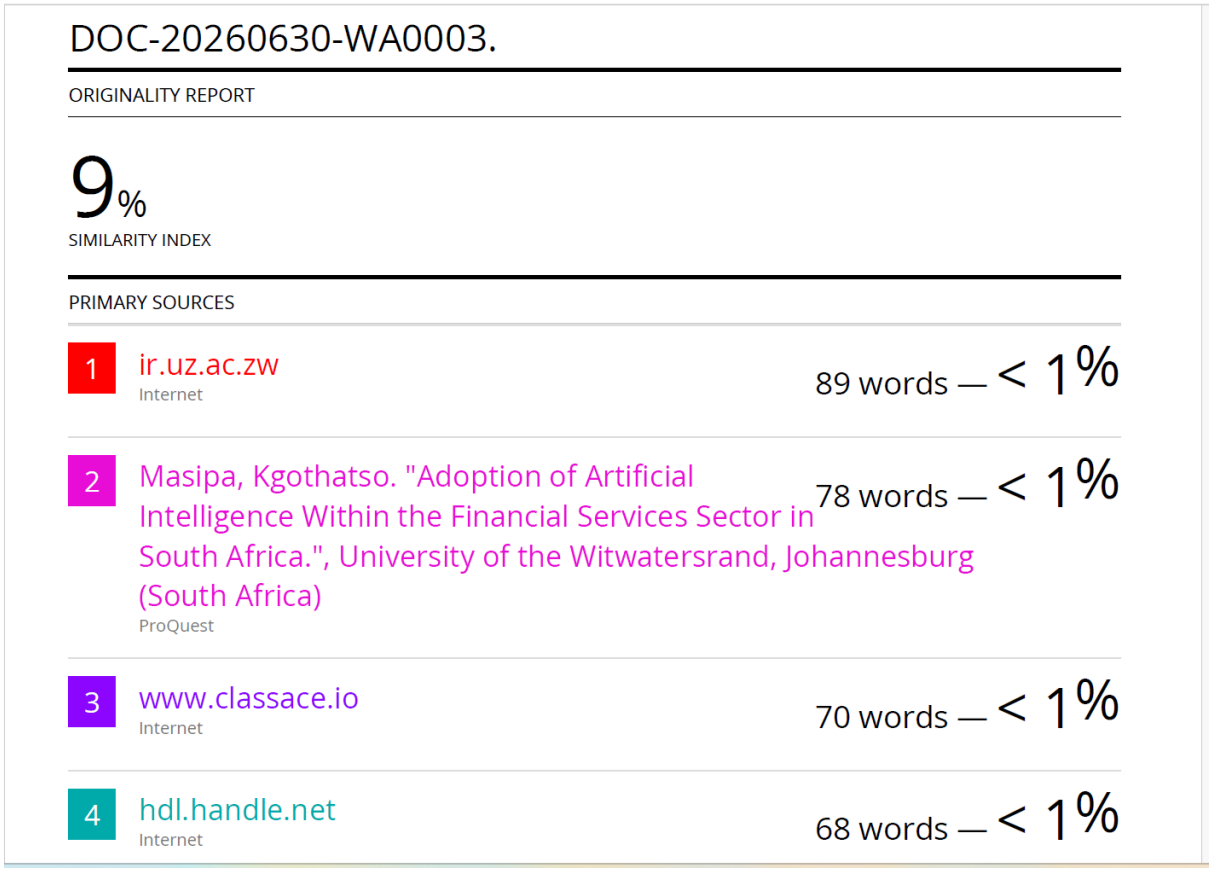
Thank you for your time

APPENDIX 2: INTERVIEW GUIDE

INTERVIEW GUIDE

1. How are cyber risk governance frameworks structured and implemented in your organisation?
2. To what extent do these frameworks support effective management of cyber risks?
3. How does senior management or the board participate in cyber risk governance within your organisation?
4. In your view, how does leadership involvement influence cybersecurity decision-making and priorities?
5. What organisational challenges affect leadership accountability in managing cyber risks?
6. How do factors such as resources, skills, or organisational culture impact cyber risk governance?
7. How are cyber risk governance practices adapted to the Zimbabwean financial services environment?
8. What improvements would you recommend to make cyber risk governance frameworks more relevant to your context?
9. How would you describe the effectiveness of cyber risk governance in your organisation?
10. What factors contribute most to strengthening cyber risk governance outcomes?
11. What role do you believe leadership accountability should play in improving cyber risk governance in Zimbabwe's financial services sector?

APPENDIX 3: SIMILARITY REPORT



DOC-20260630-WA0003.

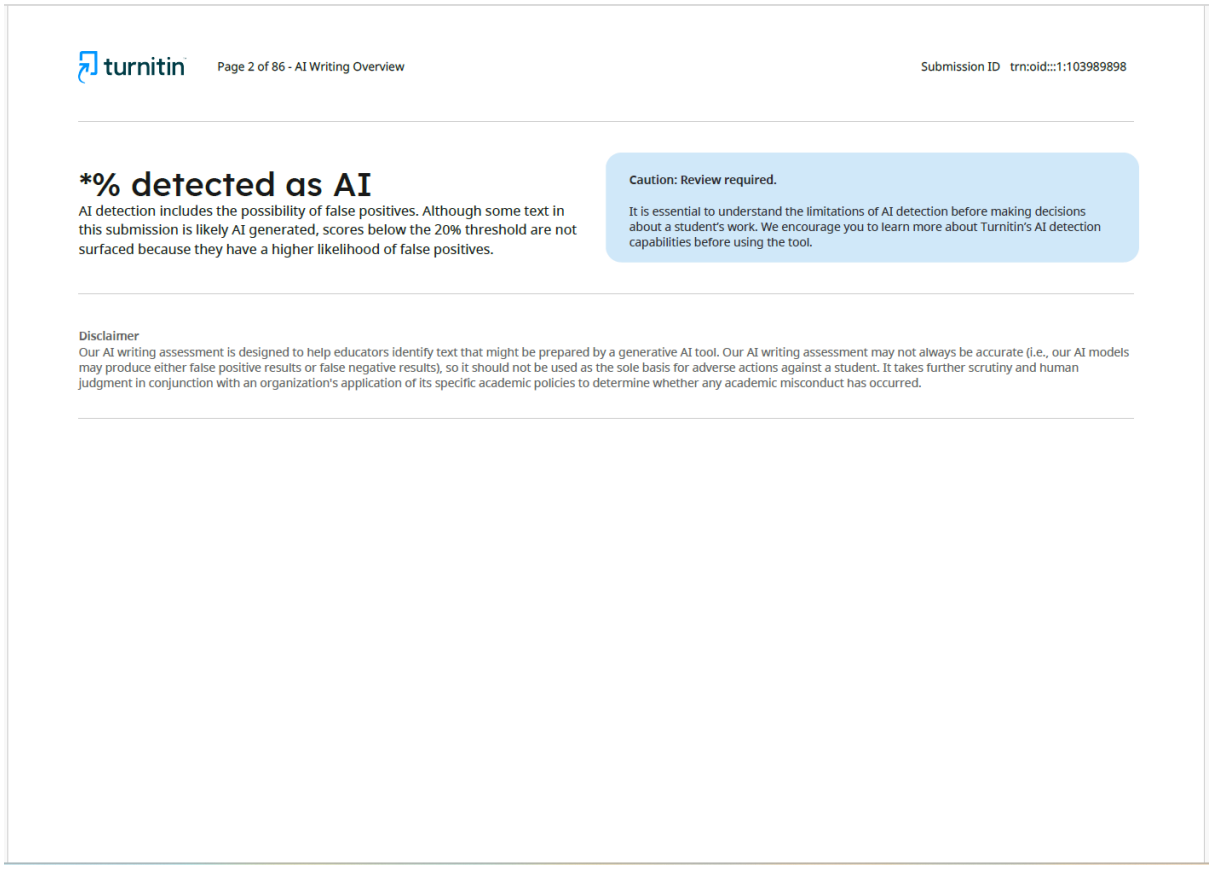
ORIGINALITY REPORT

9%
SIMILARITY INDEX

PRIMARY SOURCES

1	ir.uz.ac.zw Internet	89 words — < 1%
2	Masipa, Kgothatso. "Adoption of Artificial Intelligence Within the Financial Services Sector in South Africa.", University of the Witwatersrand, Johannesburg (South Africa) ProQuest	78 words — < 1%
3	www.classace.io Internet	70 words — < 1%
4	hdl.handle.net Internet	68 words — < 1%

APPENDIX 4: AI DETECTION REPORT



turnitin Page 2 of 86 - AI Writing Overview Submission ID trn:oid:::1:103989898

*% detected as AI

AI detection includes the possibility of false positives. Although some text in this submission is likely AI generated, scores below the 20% threshold are not surfaced because they have a higher likelihood of false positives.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Disclaimer

Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (i.e., our AI models may produce either false positive results or false negative results), so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

APPENDIX 5: ETHICAL CLEARANCE LETTER

RESEARCH ETHICS COMMITTEE

P. Bag 1020
BINDURA, Zimbabwe
Email : rid@buse.ac.zw

BINDURA UNIVERSITY OF SCIENCE EDUCATION [BUSE]

9 June 2026

Clemence Chikombingo
Bindura University of Science Education
Graduate School of Business
P. Bag 1020
Bindura

Dear Clemence Chikombingo

RE: INSTITUTIONAL RESEARCH COMMITTEE ETHICAL CLEARANCE-APPROVAL NUMBER: BUSEREC/0162/2026

Your application for research ethical clearance related to the topic **'TOWARDS LEADERSHIP ACCOUNTABILITY ON CYBER RISK GOVERNANCE IN THE FINANCIAL SERVICES SECTOR IN ZIMBABWE'** has been approved and allocated approval Number: **BUSEREC/0162/2026**. You are to quote this approval number for all correspondences inclusive of consent forms and any other documents as and when appropriate. The approval period is as stated below:

Type of Meeting	:	19th Research Ethics Committee
Approval Date	:	09/06/2026
Expiry date	:	08/06/2027

The project will automatically discontinue on the expiry date. You can apply for renewal three months before the expiry date. The renewal application should be accompanied by a progress report.

You are not expected to make any changes/adjustments to the protocol including the consent documents. Any trials involving drugs, devices and biologics require approval of the Medicines Control Authority of Zimbabwe before commencement. All problems to do with the safety of participants must be reported to BUSEREC within three (3) working days.

Upon termination of the study, a report has to be submitted to BUSEREC.

Yours sincerely

BUSEREC CHAIRPERSON