A Proposed Framework That Enhances the Quality of Cyber Security Audits

A dissertation presented to the

Department of Information Systems

University of Cape Town

By

Matsikidze Hezel

Supervised by: Professor Michael Kyobe

February 2022

In partial fulfilment of the requirements for the degree:

Master’s in information systems

DECLARATION

I, **Hezel Matsikidze**, hereby declare that the work on which this thesis is based is my original work (except where acknowledgements indicate otherwise) and that neither the whole work nor any part of it has been, is being, or is to be submitted for another degree in this or any other University. I authorize the University to reproduce for the purpose of research either the whole or any portion of the contents in any manner whatsoever.

Signature: …………H.MATSIKIDZE…. Date: ....02/02/2022……

Plagiarism Acknowledgment:

1. I know that plagiarism is wrong. Plagiarism is to use another's work and to pretend that it is one's own.

2. I have used the American Psychological Association (APA) convention for citation and referencing. Each contribution to, and quotation in this dissertation **"A proposed framework that enhances the quality of cyber security audits"** from the work(s) of other people has been attributed and has been cited and referenced.

3. This dissertation "**A proposed framework that enhances the quality of cyber security audits**" is my own work.

4. Part of this dissertation is contained in one of my published conference paper titled "A proposed cyber security framework for auditing in financial institutions".

5. I have not allowed, and will not allow anyone, to copy my work with the intention of passing it off as his or her own work.

6. I acknowledge that copying someone else's assignment or essay, or part of it, is wrong, and declare that this is my own work.

Signature: Signed by candidate

Date: 02/02/2022…………………

Full Name of Student: HEZEL MATSIKIDZE

Student Number: MTSHEZ001

ABSTRACT

The need to protect information systems or assets remains crucial today. Innovations in technology have led to rapid developments and as technology continues to advance, so is the need to protect information systems. Amongst numerous effects of cyber-attacks on organizations, huge financial losses which in turn affect the economy have since been reported. Cyber security audits need to be strengthened to tighten the protection of information systems. The importance of cybersecurity audits is widely endorsed in literature. Nonetheless, frameworks used to audit cybersecurity are viewed as 'sometimes' weak links to cyber security due to their drawbacks in auditing cyber security.

A review of literature indicated that cyber-attacks are more rampant in the African continent with the financial sector being the most targeted. Literature also highlighted that the use of relevant frameworks for auditing cyber security improves the quality and effectiveness of audits thereby enhancing cyber security. Studies in information systems have mostly looked at the adoption of frameworks, types of cyber threats and tools needed to audit. Nonetheless, it is important to note that few scholars have examined the applicability and effectiveness of the existing frameworks in auditing cyber security. Furthermore, previous studies emphasize on enhancing cyber security without a particular focus on auditing cyber security including assessing the role of the auditor during the process. As a result, this study looked at cyber security from an auditing perspective with a particular focus on the strengths and weaknesses of the current frameworks that are being used to audit cyber security including. The study also looked at the factors that enhance the effectiveness of cyber security audits.

The study draws from different theories, literature and from the strengths and drawbacks of existing frameworks to create an explanatory model. To statistically test and evaluate the model, a quantitative research approach was employed to collect, analyze, and interpret data from South Africa. Data was collected using a questionnaire which was distributed to IT auditors and cyber security professionals from the Information Systems Audit and Control Association (ISACA) South African chapter members.

The National Institute of Standards and Technology (NIST) cyber security framework was found to be the widely adopted framework followed by the International Organization for Standardization (ISO) standards, with the Control Objectives for Information Technologies (COBIT) being the least employed framework. The COBIT framework was found to be more aligned to Information Technology governance rather than cyber security. Furthermore, results of this study indicate that effectiveness of cyber security audits is dependent upon competencies of auditors including their ethics and integrity. Results further indicate that frameworks used for auditing are effective to some extent if properly implemented. A proper alignment of an auditor's competencies which include ethics and integrity, and an adoption of a relevant framework will result in effective cyber security audits that reduce the risks of cyber-attacks.

Concerning the contribution to practice, results from this study can help organizations to determine and review focus areas of cyber security auditing that they need to emphasize and develop on. Furthermore, the developed model can be used by auditors to develop an audit plan and conduct audits that are effective in identifying, protecting, detecting, preventing, and recovering information systems or assets. The methodological, theoretical, and practical contributions are further discussed in this thesis along with limitations, recommendations, and areas for future research.

Keywords: Cyber security, Frameworks, IT auditing, Information assets, Information systems

ACKNOWLEDGEMENT

Throughout the writing of this dissertation, l have received relentless support and assistance from a special set of people. I would like to express my gratitude to my supervisor Professor Michael Kyobe. His dedication, expertise and motivation pushed me to sharpen my intellectual aptitude and brought my work to a higher level.

I would also like to acknowledge my friends, family and cohorts who were always there for me to provide stimulating conversations, as well as necessary distractions to refresh my mind outside of this research.

My deepest appreciation goes to the ISACA board, including all IT auditors and cyber security professionals who participated in my research study and ensured my dissertation was a success, thank you for being a part of my journey, your valuable contribution is much appreciated.

Finally, l gratefully appreciate the funding that l received in my second year of study from the NRF. Your financial support enabled me to focus on my studies without having to worry about my finances, l am forever thankful.

DEDICATION

To the Most High God, the author and finisher of my work. To my family, your prayers and support encouraged me to work harder and achieve more accolades.

"Psalms 127: Except the LORD builds a house, they labor in vain those that build it….."

TABLE OF CONTENTS

DECLARATION i

ABSTRACT ii

ACKNOWLEDGEMENT v

DEDICATION vi

LIST OF TABLES xv

LIST OF FIGURES xvii

LIST OF APPENDICES xviii

LIST OF ACRONYMS xix

CHAPTER 1 INTRODUCTION 1

1.1 Background and statement of the problem 1

1.2 Problem statement 2

1.3 Research question 3

1.4 Research sub-questions 3

1.5 Research objectives 3

1.6 Chapter Outline 4

CHAPTER 2 LITERATURE REVIEW 6

2.1 Introduction 6

2.2 Information technology auditing 7

2.3 The role of an auditor 8

2.3.1 The lending credibility theory 8

2.3.2 The Policeman theory 9

2.3.3 The role theory 10

2.4 Cyber security 11

2.5 Defence in-depth theory 12

2.6 Agency theory 12

2.7 Strategic choice theory 13

2.8 Cyber security frameworks.. 13

Figure 2. 1: Primary frameworks used to define Cyber-security Approach in Organizations 14

Source: Jamison, J., Morris, L., & Wilkinson, C. (2018).. 14

2.8.1 COBIT5 (2012) 15

Figure 2. 3: COBIT 5 Principles (ISACA, 2015) 16

2.8.2 NIST cyber security framework 17

The framework core 18

Figure 2. 4: NIST framework implementation tiers 19

2.8.3 ISO 27000 family of standards... 21

2.8.4. Trust Service Criteria 21

2.9 Summary of literature... 23

2.10 Gaps in the literature 23

2.11 Conceptual model 25

2.12 Definition of Constructs and hypotheses 25

Table 2. 1: Definition of constructs 25

2.13 Hypotheses 26

CHAPTER 3 RESEARCH METHODOLOGY 28

3.1 Introduction 28

3.2 Philosophical consideration 28

3.2.1 Ontology 28

3.2.2 Epistemology 29

3.3 Research method 30

3.4 Research Purpose 30

3.5 Approach to theory development 30

3.6 Research Strategy 31

3.7 Research time frame 31

3.8 Data collection and process 31

3.8.1 Target population and sample 32

3.8.2 Sampling technique 32

Table 3. 1: Population and sampling 33

3.8.3 Data collection method and analysis 33

3.8.4 Data analysis ... 34

3.9 Research instrument design ... 35

Table 3. 2: Structure of the questionnaire ... 35

3.9.1 Resources and plan ... 35

3.10 Ethical considerations ... 36

3.11 Research design summary ... 37

CHAPTER 4 ... 38

DATA ANALYSIS, PRESENTATION AND DISCUSSION ... 38

4.1 Introduction ... 38

4.2. Data cleaning ... 38

4.3 Response rate ... 39

Table 4. 1: Response rate ... 39

4.4 Pilot Study ... 39

4.5 Reliability statistics ... 40

Table 4. 2: Reliability statistics for the Audit Framework construct ... 40

Table 4. 3: Reliability statistics for the competencies of auditors construct ... 41

Table 4. 4: Reliability statistics of an auditors ethics and integrity construct ... 41

Table 4. 5: Reliability of quality cyber security audits construct ... 41

4.6 Demographics and background information of participants ... 41

4.6.1 Age range of participants ... 41

Table 4. 6: Age of respondents 42

4.6.2 Levels of education 42

Table 4. 7: Participants' highest level of education 42

Source: Primary data (2021) 42

4.6.3 Certifications held 43

Table 4. 8: Certifications 43

Source: Primary data (2021) 43

4.6.4 Job title 43

Table 4. 9: Job title 43

Source: Primary data (2021) 44

4.6.5 Job industry 44

Table 4. 10: Job industry 44

Source: Primary data (2021) 45

4.6.6 Years in the profession 45

Table 4. 11: Years in profession 45

Source: Primary data (2021) 45

4.6.7 Location of business 46

Table 4. 12: Business location 46

4.7 Cyber security Frameworks 46

Table 4. 13: Cyber security audit frameworks 46

Source: Primary data (2021) ... 47

4.8 Descriptive of study variables ... 47

Table 4. 14: Descriptive statistics ... 48

Source: Primary data (2021) ... 48

4.9 Normality Tests ... 49

Table 4. 15: Normality tests ... 50

Source: Primary data (2021) ... 50

4.10 Correlation Analysis ... 50

Table 4. 16: Correlations ... 51

Source: Primary data (2021) ... 51

4.11 Linear regression analysis of cyber security audit quality against each independent variable 52

4.11.1 Framework adoption against cyber security audit quality ... 52

Table 4. 17: Model Summary ... 52

Table 4. 18: ANOVA ... 53

Table 4. 19: Regression coefficients ... 53

4.11.2 Competencies of auditors against quality cyber security audits ... 54

Table 4. 20: Model Summary ... 54

Table 4. 21: ANOVA ... 54

Table 4. 22: Regression coefficients ... 54

4.11.3 Auditors Ethics and integrity of professionals against quality cyber security audit 55

Table 4. 23: Model Summary 55

Table 4. 24: ANOVA 56

Table 4. 25: Regression coefficients 56

4.12 Regression model 57

4.13 Multi-regression analysis 57

Table 4. 26: Model summary 57

Table 4. 27: Anova 58

Source: Primary data (2022) 58

Table 4. 28: Regression coefficients 58

Source: Primary data (2022) 58

4.14 Conclusion 59

CHAPTER 5 60

SUMMARY, CONCLUSION AND RECOMMENDATIONS 60

5.1 Introduction 60

5.2 Summary of findings 60

5.3 Research objectives and findings 60

5.4 Conclusion 61

5.5 Recommendations 62

5.6 Areas for further study 63

REFERENCES.. 64

APPENDICES.. 75

LIST OF TABLES

Table 2. 1: Definition of constructs..25

Table 3. 1: Population and sampling..33

Table 3. 2: Structure of the questionnaire 35

Table 3.11: Research design summary…………………………………………………..37

Table 4. 1: Response rate 39

Table 4. 2: Reliability statistics for the Audit Framework construct.......................................40

Table 4. 3: Reliability statistics for the competence of audit personnel construct..................41

Table 4. 4: Reliability statistics of the ethics construct...41

Table 4. 5: Reliability of the internal cyber security factors construct 41

Table 4. 7: Age of respondents...42

Table 4. 8: Participants' highest level of education 42

Table 4. 9: Certifications 44

Table 4. 10: Job title...45

Table 4. 11: Job industry 45

Table 4. 12: Years in profession..46

Table 4. 13: Business location...47

Table 4. 14: Cyber security audit frameworks 44

Table 4. 15: Descriptive statistics..49

Table 4. 16: Normality tests 48

Table 4. 17: Correlations 49

Table 4. 18: Model Summary... 50

Table 4. 19: ANOVA 50

Table 4. 20: Regression coefficients 51

Table 4. 21: Model Summary... 52

Table 4. 22: ANOVA 52

Table 4. 23: Regression coefficients 52

Table 4. 24: Model Summary... 53

Table 4. 25: ANOVA 54

Table 4. 26: Regression coefficients 54

Table 4. 27: Model summary 55

Table 4. 28: Anova... 56

Table 4. 29: Regression coefficients 56

.

LIST OF FIGURES

Figure 1. 1: An illustration of the dissertation structure 5

Figure 2. 1: Primary framework used to define Cyber-security Approach 14

Figure 2. 2: 2019 Global IT Audit benchmarking survey 15

Figure 2. 3: COBIT 5 Principles 16

Figure 2. 4: NIST framework implementation tiers 19

Figure 2. 5: A framework for enhancing the effectiveness of quality cyber security audits….25

LIST OF APPENDICES

APPENDIX A: RESEARCH INSTRUMENT...75

APPENDIX B: CONSENT FORM AND COVER LETTER…..80

APPENDIX C: ETHICS CLEARANCE FORM… 81

APPENDIX D: DATA COLLECTION APPLICATION..82

APPENDIX E: ISACA DATA COLLECTION APPROVAL LETTER AND EMAIL......... 86

LIST OF ACRONYMS

1. IT – Information Technology
2. IIA – Institute Of Internal Auditors
3. IS – Information Systems
4. ISACA – Information Systems Audit And Control Association
5. ISMS – Information Security Management Systems
6. ISO – International Organization For Standardization
7. CISA – Certified Information Systems Auditor
8. CISSP – Certified Information Systems Security Professional
9. CIA – Certified Internal Auditor
10. COBIT- Control Objectives For Information Technology
11. NIST- National Institute Of Standards And Technology
12. TSC – Trust Service Criteria

CHAPTER 1

INTRODUCTION

This is an introductory chapter which discusses the problem statement and the background of the study. It further develops into the research objectives, research questions and lastly, it illustrates how the rest of the thesis is structured.

1.1 Background and statement of the problem

In the past few decades, there has been a revolution in computing and communications and all indicators are that technological progress and use of information technology will continue (Tarek, Mohamed, Hussain & Basuony, 2017). Otero (2019) and Bozkus Kahyaoglu & Caliyurt (2018) agree that the revolution in information and communication technology has changed not only human lives but has had a great impact on business operations. According to Tarek *et al.,* (2017), information technology has shaped how businesses reach more customers, product development and services as well as customer suppliers and business partners' collaboration. The authors added that the interdependence of business systems and information technology birthed information technology auditing as means to evaluate systems put in place to mitigate losses resulting from cyber-crimes.

Over the past decade, Information technology auditing has grown to be a crucial part of every institution. This can be accredited to the ability of an IT audit to reduce risks by examining implemented cyber security policies, controls and procedures, to mention but a few (Jreissat, Gall, & Doheir, 2018). According to Kolk (2017), two professions of Information technology and accounting (auditing) were the main contributors to the development of IT auditing including the frameworks used. As can be seen in all sectors world over, the financial industry has largely benefited from the development of information technology audits, performed through the use of relevant cyber security frameworks.

Scholars including Otero (2019) and Kshetri (2019), noted that the African financial service sector, which is mainly dominated by banks, is arguably the most fragile and contagious sector as compared to other different business sectors cyber security wise. In that regard, this makes the sector one that is closely guarded by authorities to ensure stability (Kshetri, 2019). To add on, Kshetri (2019) noted that the rate of cybercrime is on the rise in developing countries in

Africa more than in any other area in the world which is a call for concern. He accredited this to poor cybercrime legislations, under-skilled professionals, vulnerable systems and lack of proper cyber security guidelines, practices and policies making Africa a haven for cybercriminals to function with impunity. According to Kshetri (2019), in Africa, banks are more prone and are at high risk from cyber threats such as hacking, malicious insiders and data breaches. One study that was conducted by Deloitte in African banks revealed that 60% of the investigated banks had insecure systems and they lacked appropriate cyber security practices. According to the South African Banking Risk Information Centre, the Republic of South Africa loses around $157 million annually to cyber-attacks. To echo these findings, in 2014, the United Nations Economic Commission for Africa (UNECA) noted that in Africa, cyber security was seen as a luxury and not a requisite whilst one major mechanism that can ensure the continued effectiveness of cyber security is auditing.

As a result, this study aims to look at cyber security from an auditing perspective in South African financial institutions. This research gives practical insights on the current cyber security posture of financial institutions, drawbacks of existing frameworks that are used for cyber security auditing, factors that enhance cyber security and finally, an explanatory framework presented.

1.2 Problem statement

The continuous rise of cyber threats in South African financial institutions leads one to question the effectiveness of cyber security audits. Cyber threats have been a contributing factor to the demise of the economy hence a need to curb this problem (Kshetri, 2019). Literature accredited the use of frameworks in strengthening audits and as such, scholars have given critique on the existing frameworks on their applicability to auditing cyber security (ISACA & Protiviti, 2020; Jreissat *et al*., 2018; Otero, 2019; Yeboah, 2013). Some scholars argue that the reason for the aforementioned lies in the drawbacks of the current frameworks that are being used for cyber security auditing (Otero, 2019). Furthermore, literature on the existing frameworks mainly comes from surveys and studies conducted in other continents besides Africa whilst the African financial sector is at high risk of cyber threats more than any other continent (Kshetri, 2019). For this reason, a framework that identifies factors that enhance the effectiveness of cyber security audits was proposed.

1.3 Research question

The research question to be answered by this study is, *'What factors influence the performance of quality and effective cyber security audits in South African financial institutions?'*

1.4 Research sub-questions

In answering the main research question above, the following sub-research questions are dealt with:

a) What are the strengths and weaknesses of the existing frameworks in auditing cyber security in financial institutions?
b) How effective are the current frameworks in auditing cyber security?
c) To what extent does an auditors skills contribute to the quality and effectiveness of audits?
d) To what extent does ethics and integrity of an auditor assist in ensuring quality and effective cyber security audits?

1.5 Research objectives

To answer the proposed research questions, the objectives of the study are to:

- Evaluate the current frameworks used for cyber security auditing in financial institutions.
- Analyze the current cyber security audit processes and security posture of financial institutions.
- To determine the effectiveness of audits in reducing cyber threats including the role of an auditor in the process of auditing.
- To determine the factors that influence the performance of effective and quality cyber security audits

1.6 Chapter Outline

This dissertation is structured into 5 chapters as below.

Chapter 1 – Introduction: This introductory chapter discusses the problem statement and the background of the study. It further develops into the research objectives, research questions and lastly, it illustrates how the rest of the thesis is structured.

Chapter 2 - Literature Review: Chapter 2 explicates the existing literature. It introduces and explains the aspect of IT auditing, cyber security and gives a critical analysis of the existing frameworks namely COBIT, ISO standards, NIST cyber security framework and the Trust Service Criteria. Lastly, a conceptual model was developed and discussed.

Chapter 3 - Research Design: This section outlines the research philosophy, the research method, strategy, and time frame. The chapter explains how the sample for the study was selected. It also explains how the research instrument used in the study was designed and the ethical considerations that were made before data was collected.

Chapter 4 - Data Analysis, Findings and Discussion: This chapter provides a demographic and descriptive analysis of the data collected. Regression analysis and correlation analysis are used in the study. Findings and their discussion thereafter are also provided in this chapter.

Chapter 5 - Conclusion and Recommendations: Chapter 5 concludes the dissertation. It provides a summary of the results or findings and outlines the contributions of the study and recommendations for future research.

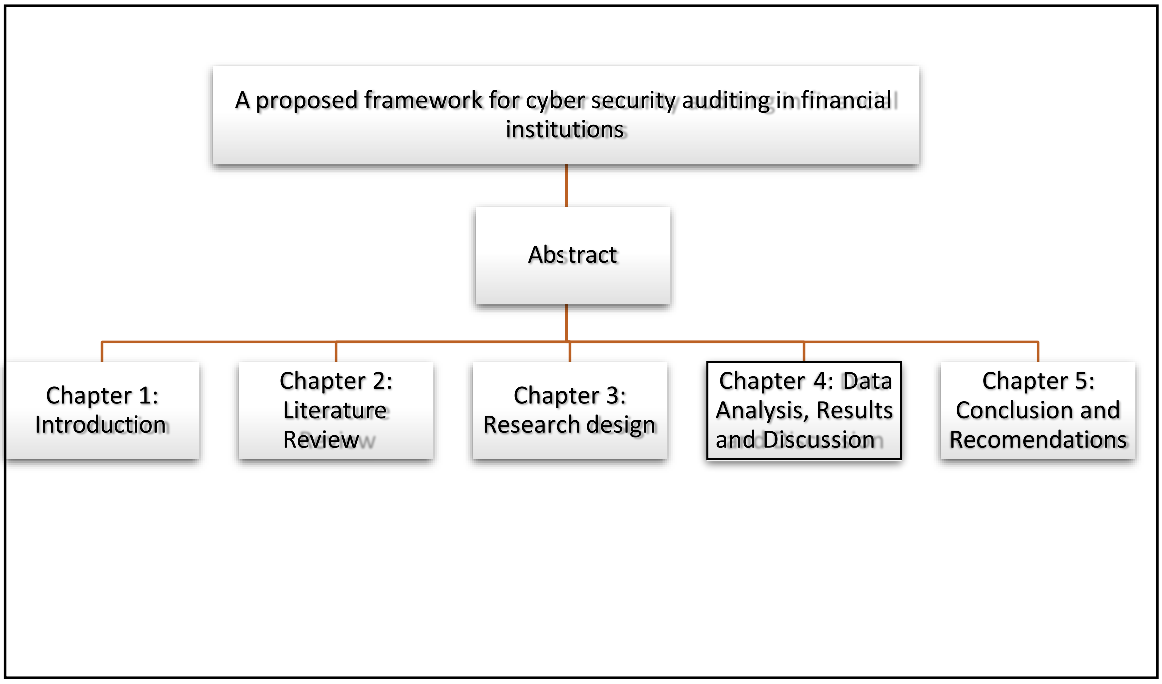

Figure 1. 1: An illustration of the dissertation structure

CHAPTER 2

LITERATURE REVIEW

This chapter illustrates a critical analysis of existing literature, scholarly arguments, and theories relevant to the subject of enquiry of this research. Based on the literature review, a conceptual model was developed, and hypotheses presented. This literature review provides insight into information technology auditing, cyber security including cyber security frameworks and explores different theories underlying the study. It further highlights the gaps in literature and presents the conceptual model that was developed for this study.

2.1 Introduction

In recent years, given the rapid developments in technology and its impact on the business environment, the need to ensure data protection led practitioners and researchers to focus on information technology auditing (Asfaw, 2018). Information technology auditing includes implementing mechanisms that ensure IT risks which mostly constitute cyber threats are duly mitigated, and systems are performing as expected towards achieving organizational goals. To ensure data protection, there is a need for auditing including ‘good’ cyber security practices (Tariq, 2018). Past literature has confirmed that cyber threats are more rampant in African financial institutions (Kshetri, 2019; Tariq, 2018; Borghard, 2018). Much of this has been attributed to poor regulatory policies, poor cyber security practices and lack of watertight organizational security standards making the African financial sector a haven for cyber hackers to operate (Kshetri, 2019; United Nations. Economic Commission for Africa, 2014). The African financial sector has no clear regulations and laws that initiate compliance to cyber security frameworks hence organizations willing to cement their cyber security have had to rely on international practices such as ISO standards, COBIT and Trust Service Criteria (TSC) (Islam, Farah, & Stafford, 2018). Furthermore, there is a need for financial institutions to protect the interests of shareholders and third parties and it has been said that the ongoing damage caused by cyber threats has made shareholders question the effectiveness of audits performed (Asmah, 2019). Literature accredited good practice of cyber security to the use of available cyber security frameworks and performing regular audits (Islam et al., 2018). As such, this study aims to critically evaluate the most accredited cyber security frameworks from an auditing perspective and to develop a framework that identifies factors that aid in improving the effectiveness of cyber security audits in financial institutions.

2.2 Information technology auditing

The term ‘audit’, according to the Information Systems Audit and Control Association (2015), alludes to the formal examination and inspection to validate a standard or set of guidelines, to inspect if the standards and guidelines are being adhered to, records are precise, and targets are being met. Types of auditing include external auditing, internal auditing, financial auditing, operational and IT auditing. According to ISACA, (2015) and the Institute of Internal Auditors (IIA), (2012), the main objective of performing audits is to evaluate if the organization in question is complying with regulatory requirements, to assess the strategic and financial position of the organization and to identify risks or weaknesses that management has otherwise failed to see. This means that the role of auditors is about detecting where proficiencies can be made through innovations. It is about reviewing risk management including processes to evaluate whether the right processes exist and how they can be improved to put the organization in a better position to achieve its objectives (IIA, 2018; Matsikidze and Kyobe, 2020).

Information technology (IT) is epitomized by three fundamental components namely people, process, and IT (Lloyd, 2020). It deals with strategic, managerial, and operational activities involved in overseeing data (Jamison, Morris & Wilkinson, 2018; Otero, 2019; Susana & Pereira, 2018). IT also involves the hardware, software, communication, and other amenities necessary to manage information that is input, storage, processing, and output (Avgerou & Walsham, 2017). The IT auditing profession was birthed from different professions namely auditing (accounting) and information technology (Mihret & Grant, 2017). In combining both definitions above, IT auditing is defined as the official, liberated, and objective inspection of an organization’s IT infrastructure to regulate whether the activities involved in gathering, processing, storing, transmitting, and utilizing information comply with guiding principles, safeguard assets, maintain data integrity and operate effectively and efficiently to achieve an organization’s overall goals (ISACA, 2019; Osamah *et al.*, 2018; Otero, 2019). Its main objective is to check and evaluate internal controls to minimize business risks. Similarly, a cyber security audit is a thorough review and examination of an organizations information technology infrastructure to identify threats, vulnerabilities, risks and weaknesses (Wertheim, 2019). The main goal of a cyber security audit is to identify, protect, detect, respond and recover information assets which is a significant role in helping organizations prevent cyber threats (Wertheim, 2019). According to Deloitte (2017), a successful or quality audit commences with a thorough evaluation of the IT environment, understanding the IT risks and resources required to carry out the audit. This means that the audit scope and objective of the audit is defined (Wertheim, 2019). Secondly, the audit scope is set. According to Deloitte (2017), setting the audit scope means identifying all aspects to be considered in the audit including limitations. It is important to note that cyber security audits are more restricted in scope due to the technical detail and complexity to be covered. The next step will be to determine the audit procedures. At this stage, enough data should have been gathered to enable the auditors to commence with the audit strategy and audit program. It is at this stage that testing steps should be defined. According to Sabillon, (2018), testing steps and the framework to be used should be adjusted so as to be relevant to a specific organization being audited based upon risk. The auditor(s) to conduct the audit should also have relevant skills and knowledge so they may be able to conduct a thorough audit that produces quality results. This is so because failure to adjust may result in an auditor recommending controls that are not relevant to the organization resulting in an audit that does not improve an organizations' cyber security (Deloitte 2017; ISACA, 2017; Sabillon, 2018). This highlights how important the framework used to audit is, an auditor's skills and the audit objective.

To further understand more of the aforementioned, it is important to understand the main role of an auditor and their contribution to cyber security audits. The following section seeks to understand the role of an auditor through the use of relevant theories.

2.3 The role of an auditor

The following theories explicate the role of an auditor.

2.3.1 The lending credibility theory

In conducting business, investors and lenders face a risk regarding their investments. An audit report of a company directly influences investors and lenders business decisions (Axelsen, Green, & Ridley, 2017). The lending credibility theory stipulates that the audit role emanated from the need to add credibility to a company's financial statements (Ittonen, 2010). It further adds that auditors serve the sole purpose of cementing assurance and confidence that a company's financial statements have been correctly prepared with ethics and integrity in accordance with the accepted principles and statutory provisions (Jizi, Salama, Dixon, and Stratling, 2014; Ittonen, 2010).

Recent reports in South Africa have indicated a decline in the quality of audits performed by auditing companies notably the Big four accounting firms (Deloitte. PwC, EY, KPMG) (Agyemang & Badai, 2020). Public cases to note are the bankruptcy of Lehman brothers' investment bank in which the corporations and crime report noted that Ernest and Young did not reveal fraud involved leading to the demise of the bank (Agemang & Badai, 2020). As a result, this has eroded public trust and confidence in auditors or auditing. A report by the Corporations and Crime Report (2020) portrays auditors as more willing to please clients by rubber-stamping inaccurate financial statements, rather than serving the interests of the public and the economy in which they operate (Agemang & Badai, 2020).

Another case to note is when a credit card company called PayGate was hit by a cyber-attack in August 2012 (Van Niekerk, 2017). It was reported that four major banks of South Africa were affected and it resulted in the banks suffering huge financial losses (Van Niekerk, 2017). In line with the lending credibility theory, such events question the credibility of cyber security audits, the auditors and the organization itself. Jibrin, Blessing, & Danjuma (2014), further states that "Such events raise questions about the value of company audits, auditor independence and the quality of audit work. (p. 231)" This places value and reliance on auditors' skills, ethics and integrity to ensure quality audits.

IT auditing is a vastly valued service as it provides insights into management integrity and ethics including the level of risks to make a difference into an entity's operations (Mahzan & Hassan, 2015). Increasingly due to cybercrimes, there is a high interest in the need for quality cyber security audits that go beyond mere audits of financial statements (IIA, 2010). Clients of corporate organizations including investors and stakeholders presently do not just request more accountability and transparency with financial statements, they likewise request affirmation that the organization is forcefully controlling risks contributed by IT use, complying with regulatory requirements and the executives' steps to secure key business assets (Otero, 2019).

2.3.2 The Policeman theory

The policeman theory claims that the main role of an auditor is to detect and prevent fraud (Halbouni, 2015). This has been a debate as some scholars dispute the policeman theory claim and posit that an auditor should focus on revealing an organizations financial position rather than having fraud detection as the main role (Hay, 2014; Owolabi, & Olagunju, 2020). Adding to that is the agency theory which postulates that audit services emancipate from both the interests of the third parties (shareholders, suppliers, etc.) and management. The theory explains the underlying relationship between the principles (third parties) and the agent (management). Where decision making is mostly done by the agent, mistrust and conflict arise where the agent may make decisions in their favour which may be a disadvantage to the principle (Shi, Connelly, & Hoskisson, 2017). Auditors thereby act as a monitoring system for principles to gain trust and a reliable opinion on the financial statements or decisions made by the agents (Panda & Leepsa, 2017). This theory asserts the role of auditors as a confirmation in providing assurance and unbiased opinion to clients and interested parties about an organization (Hay, 2014). Stafford, Deitz, & Li, (2018) assert the role of auditors in the identification of information security threats and suggest ways of improving enterprise risk management. Deducing from the aforementioned, it can be agreed that auditing deals with the evaluation of systems and business operations to mitigate risks and ensure the organization is operating according to regulatory requirements whilst providing clients with the trust, they need to continue doing business with the ‘agent’.

It remains vague as to whether the role of IT auditors is to detect and prevent cyber threats or it is to assure cyber safety. It is the view of the author that effective auditing of cyber security requires the auditor to detect and prevent cyber threats to provide reasonable assurance of cyber safety. A question of integrity however remains where auditors are involved and facilitate the crime thereby enabling and hiding it.

2.3.3 The role theory

The role theory enacts human behaviour to their social positions or status. It posits that roles are induced as a result of expectations for role behaviour (Biddle, 2013; Hindin, 2007). Thus those who exhibit the role are stimulated to do so because they learn what behaviours are expected of them while others are stimulated through their expectations to teach and enforce appropriate behaviours for those who are members of the position (Biddle, 1986; Lapalme, Kabiwa, & Tardif, 2019). An understanding of one and others’ expectations contributes to playing a good role. How well one knows the roles is a function of ones’ previous experience and knowledge gained through observations, conversations or formal education (Biddle, 2013; Lapalme et al., 2019).

Debates central to this theory have been on what scholars refer to as the audit expectation gap. According to Ebimobowei, Kereotu & Brass (2011), this is the gap that exists between what the public (people, management and board of directors) expects from auditors and what the auditors perceive their duties to comprise of. Whilst Ebimobowei et al. (2011), portrays public trust as the core value of a profession and argues that if such trust is betrayed, the profession becomes useless, Ramsarghey and Hardman (2020), argue that societal expectations of audits are unrealistic and beyond an auditor's actual standard of performance. Prior to an auditors' role in cyber security, according to the lending credibility theory, it is the duty of the auditor to detect and prevent cyber-attacks including risk management and recovering loses from cyber-attacks.

The following section addresses cyber security and its principles including the underlying theories.

2.4 Cyber security

Cyber security is a complex issue that encompasses physical security to digital security. According to ISACA (2015), cyber security is defined as the practice of protecting information, networks, systems, and programs from cyber-attacks. Otero, (2019) also posits that cyber security is simply techniques and measures put in place to prevent cyber-attacks. Innovations in technology have introduced a shift in the financial sector from traditional banking methods to digital banking. Traditionally, it was physical theft of money to computer fraud and now it involves hacking into the system to obtain sensitive data or information (Kshetri, 2019). Innovations in technology bring forth new cyber-attacks making it difficult to ensure guaranteed security against cyber threats (Tarek et al., 2017). As a result, auditing cyber security has proven to be a challenge due to emerging technologies, rules and regulations that govern it and tools used to perform the audit (ISACA, 2019; Jamison et al., 2018: Evans, 2022). In the absence of laws compelling disclosure, it becomes difficult to measure the impact of cybercrime on the economy as most cases are left unreported and or undetected. Cybercrimes left undetected gives organizations a false sense of security and makes shareholders question the goal of auditing cyber security. Auditing cyber security in the financial organization sector has the main goal of describing the financial organization security posture, to determine its implemented controls and technologies, identify loopholes and provide a feasible solution while ensuring compliance to regulations and policies (ISACA, 2019; Jreissat et al., 2018). The financial sector is prone to attacks as the data that they hold can be siphoned for criminal activity like a fraud. Cyber threats to financial institutions include but are not limited to malware attacks, phishing, spoofing and data breaches (Osamah et al., 2018; Susana & Pereira, 2018).

Practical discussions on the motivations behind cybercrimes differ. Common motivations have been asserted to cause harm and extortion (Li, 2017). Economic theories purport that benefits drive human behaviour. This means that benefits that could come from a certain act derive an individual to behave in a certain way (Weijer, Leukfeldt, & Van der Zee, 2020). Committing a cybercrime is the main motivation behind it. Contrary to this is the intrinsic motivation theory which stipulates that the motivation behind an act is attributed merely to the interest and challenges which bring enjoyment in achieving the desired output (Brackett, Elbertson, & Rivers, 2015). It can be said that the encountered challenges in hacking give cybercriminals the satisfaction or enjoyment they need as motivation (Brackett et al., 2015). The motivation behind cybercrimes targeted at financial institutions is mostly because of benefits to be incurred including the mere satisfaction that comes with it (Brackett et al., 2015).

2.5 Defence in-depth theory

The defence in-depth theory is an approach to protecting an organizations information asset through a multilayered approach. The theory gives a focus on three main aspects that are technical controls, physical controls and administrative controls (Coole, Corkill & Woodward, 2012). It describes the underlying foundations of systems defense mechanisms that should be enforced by organizations in an attempt to secure information assets. It depicts information security as a multi-layered approach. It was designed in such a way that it has several procedures that protect detect and respond to attacks on systems. The use of Defense in Depth in IT security depends on controls that intend to delay, with almost no execution of controls focused on recognition or reaction (Coole et al., 2012). As a result, there is a need for organizations security to be aligned with the defence in depth from identification of cyber threats to the responding stage (Razana and Shafiuddin, 2016). This, theory forms a foundation for an auditing framework that aims to defend, protect, prevent and recover information assets.

2.6 Agency theory

The theory explains the underlying relationship between the principles (third parties) and the agent (management) (Panda, & Leepsa, 2017). The agency theory postulates that the principal and the agent enter into a contractual relationship that entrusts and delegates responsibility to the agent (Adams,1994; Vitolla, Raimo, & Rubino, 2020). Security-wise, this responsibility includes safeguarding information from threats, data breaches and complying with regulations. Conflict arises due to uneven distribution of data which favours the agent. The agent may break security policies for vindictive reasons or for mere convenience thus failing the principle. It is then part of the aims of security audits to prevent and expose such.

2.7 Strategic choice theory

Many information security theories assert the level of risk, environment, regulatory requirements and attitude of leaders as some of the factors that drive organizations to engage in cyber security practices (Ciborra, 1997). The strategic choice theory explains the behaviour of leaders in making a decision. It stipulates that leaders within an organization have the power to make influential decisions that allow an organization to achieve its goals. The theory further attributes characteristics of the decision makers; the environment as guiding restrictions to decision making (Ciborra, 1997). Complementing this is the notion that threats and opportunities surrounding the environment in which a business operates influence decision making. In line with the aforementioned, threats and opportunities surrounding an organization may 'force' decision- makers or agents the extent to which they engage in good cyber security practices. As financial institutions operate in an environment surrounded by threats (cyber threats), it is paramount to conduct quality and effective cyber security audits much to the benefit of the company and the 'public'.

The following section analyzes the cyber security frameworks in question.

2.8 Cyber security frameworks

Safety aspects of business and electronic transactions transfer require a more complex audit hence as a countermeasure, financial institutions saw the need of adopting cyber security frameworks which can be used for IT auditing (Jreissat et al., 2018; Osamah et al., 2018). A framework sets out the standards, guidelines, and procedures that the auditing team will audit against hence it plays a pivotal role as a driving factor to the development of the audit (Drljača & Latinovic, 2017). It is deemed vital for an auditor to take into account the organizations regulatory policies, legal requirements and standards in addition to the advantages and disadvantages of the framework when selecting a framework for an organization (Jamison et al., 2018; Kahyaoglu, and Caliyurt, 2018). A joint research by the Internal Audit Foundation and Crowe (Jamison et al., 2018), revealed the top three most used frameworks in defining a cyber security approach as the National Institute of Standards and Technology framework (NIST), Control Objectives for Information Technology framework (COBIT5) and International Organization for Standardization 2700 (ISO) respectively. This is shown in figure 2.1 below.

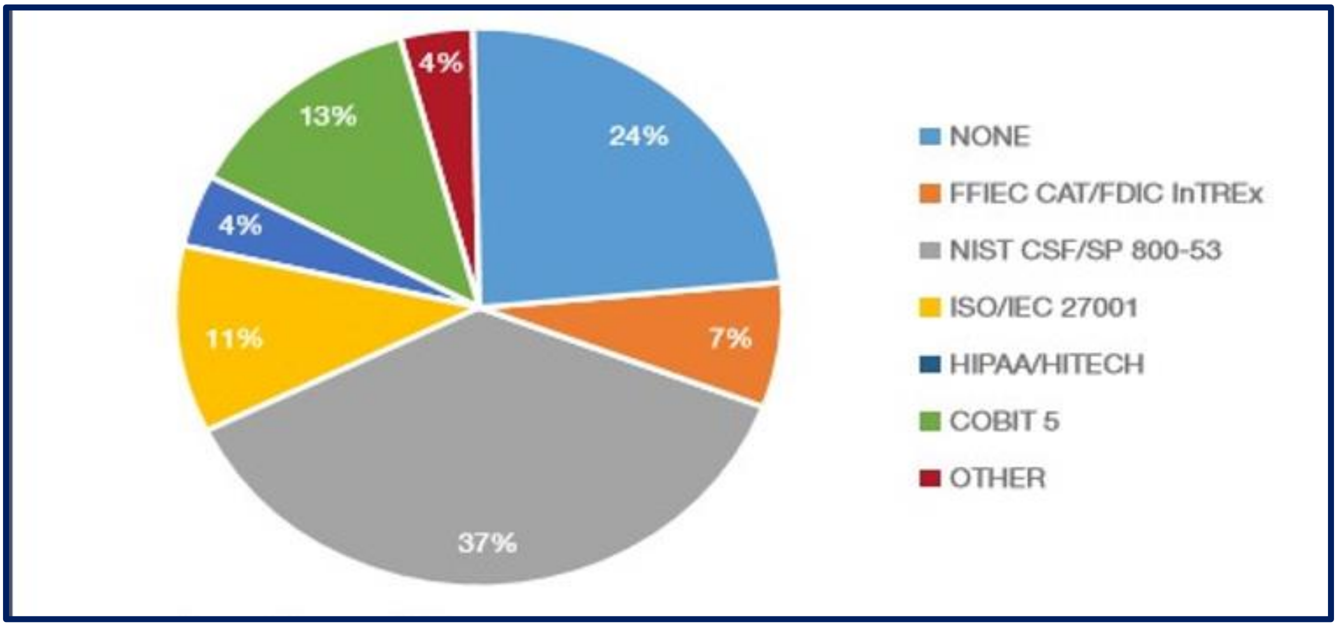

Figure 2. 1: Primary frameworks used to define Cyber-security Approach in Organizations
Source: Jamison, J., Morris, L., & Wilkinson, C. (2018)

To echo the above results, the 2019 annual global IT audit benchmarking study conducted by ISACA and Protiviti revealed statistics which show in percentages the most used framework in performing cyber security assessments in organizations. As shown in figure 2.2, it indicates the NIST cyber security framework as the most used framework and the trust service criteria framework as the least used framework and for that reason, the four frameworks were chosen for this research. The frameworks will now be discussed in detail.

Which of the following frameworks does the audit function use in performing assessments of the organization's cybersecurity posture/maturity?
(Multiple responses permitted)

	Leaders	Non-Leaders
NIST Cybersecurity Framework	64%	56%
COBIT	53%	52%
ISO 27000	47%	41%
NIST 800-53	24%	19%
CIS Top 20	12%	14%
FFIEC Cybersecurity Assessment Tool	15%	11%
AICPA Trust Service Criteria	10%	5%

Figure 2. 2 : Global IT Audit benchmarking survey
Source: ISACA and Protiviti (2020) (p.11)

2.8.1 COBIT5 (2012)

The Control Objectives for Information and Related Technologies (COBIT5) framework was developed by ISACA and according to ISACA (2015), the COBIT framework is an integrated tool that was developed to address almost all of the aspects of IT particularly IT governance. It is focused on aligning Information Technology with business. From 1992 the framework transitioned in focus from control objectives to the COBIT 3rd edition which added management guidelines (ISACA, 2015). From there came COBIT 4.0 and then 4.1 which added governance and compliance processes. Currently, the COBIT 5 version has its full focus on IT governance and management and has since been accredited as the most 'powerful', integrated framework for IT governance and control. According to Ndlovu and Kyobe (2016), the COBIT5 framework is superior to the rest as it provides a holistic approach to good IT governance practices. Furthermore, experts claim that one of the fundamental reasons COBIT has been received by such huge numbers of organizations globally is that it manages each part of IT (ISACA, 2019; Jreissat et al., 2018; Otero, 2019; Yeboah, 2013; De Haes, Van Grembergen, & Debreceny, 2013). Devos and Van de Ginste, (2014) claimed that the framework is not a scholarly framework due to the lack of theoretical work done much to the academic claims of the framework.

COBIT 5 framework has 5 principles as depicted in figure 2.3 below.

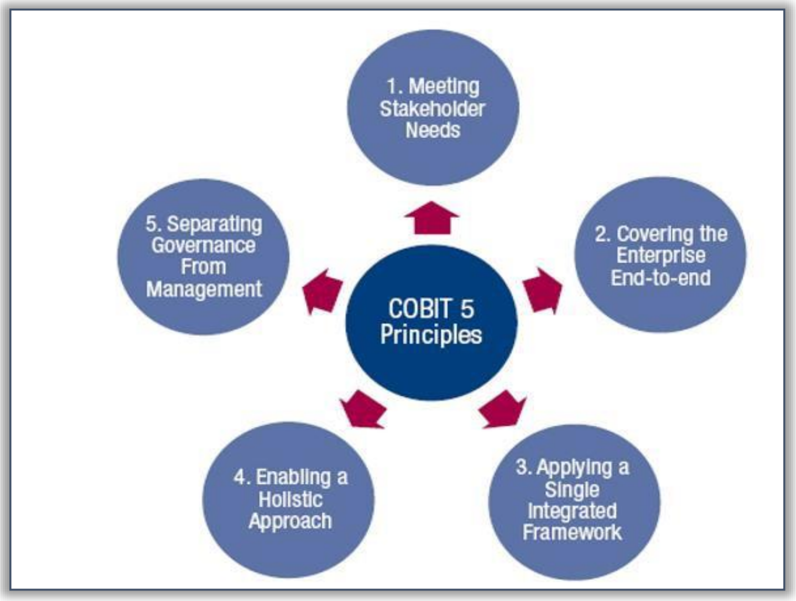

Figure 2. 3: COBIT 5 Principles (ISACA, 2015)

The framework has seven enablers as explained below according to ISACA (2015), namely, principles, policies and frameworks, processes, organizational structures, ethics, culture and behaviour, information, services infrastructure, and applications and finally people, skills and competencies (ISACA, 2015; Jreissat et al., 2018).

1. **Principles, policies and frameworks-** are the vehicle to translate the desired behavior into practical guidance for day-to-day management.
2. **Processes-** encompass an organization's set of principles and practices to achieve its objectives
3. **Organizational structures**- are the key decision-making entities in an organization.
4. **Ethics, culture and behavior**- are very critical to the success of management and governance activities.
5. **Information** – is required to keep the organization running and for the governing of the organization at large. It also includes the security of an organization’s information.
6. **Services infrastructure and applications**- encompasses the technology, applications and infrastructure that provide organizations with IT processing and services.
7. **People, skills and competencies**- required for all functions and processes to be complete and for making the correct decisions.

COBIT 2019

The latest version of COBIT framework is the COBIT 2019. It has its foundational roots in the COBIT 5 framework with a few features that were added (Steuperaert, 2019). The COBIT 2019 has six principles as compared to the five principles that the COBIT 5 has with the existing principles having been renamed. A notable enhancement to the COBIT 2019 framework is how it has been made simpler to utilize and implement through the removal of the frameworks "enablers" which were quite abstract (Steuperaert, 2019). However, although the framework can be used for performing cybersecurity audits, its core focus is on IT governance.

Prior to its credibility as an integrated/holistic framework that covers almost all aspects of IT, the framework has loosened its focus perspective from auditing to IT governance and controls (Anomah & Aduamoah, 2018). Furthermore, according to a study conducted by Steuperaert, (2019), both the COBIT5 and COBIT 2019 framework have a major drawbacks in information security specifically. Out of their numerous processes, they have only one aspect that addresses information security. Similar to this is the notion that the integrated framework COBIT 5 is too complex and therefore leaves room for generalization in other aspects like information security (Jamison et al., 2018; Steuperaert, 2019). The authors of the globally accepted framework, ISACA recommend customization of the framework to better suit the desired audit outcome. IT auditors are urged to use their experience, skills and professional judgment for the customization of the framework. However, the researcher has found this to be controversial in practice to cyber security as it presents room for generalization and vulnerabilities which is the main concern in auditing cyber security. Akin to this, another scholar indicated that most organizations do not know how to utilize and take full advantage of the "complex" framework (Susana & Pereira, 2018). This is because it requires a great deal of knowledge to understand it before it can be implemented. To add on, the institute of internal auditors' research foundation listed the COBIT framework as more business-IT aligned (IIA, 2018). They argue that the framework is a comprehensive IT governance framework and not a pure technology standard for cyber security. (Jamison et al., 2018). Aligning it to the defense in-depth theory, the framework does not allow for information assurance as it 'generalizes' the security aspect. Scholarly arguments discussed above present the framework as more of an IT governance rather than one for auditing cybersecurity.

2.8.2 NIST cyber security framework

The NIST cyber security framework was released with the aim of protecting critical infrastructure from cyber-attacks (Ibrahim, Valli, Mcateer, & Chaudhry, 2018). Organizations have since adopted the NIST cyber security framework to cement their cyber defense and mitigate risks (Ibrahim et al., 2018). The framework is designed in three parts mainly the framework core, the framework implementation tiers and the framework profile which shall be discussed. The framework core describes five functions that are based on risk management and information security namely identify, protect, detect, respond and recover (Jreissat et al., 2018; Shen, 2014).

The framework core

1. **Identify**- the identify function provides a guideline for organizations to identify security risks before asset management, business environment and IT governance through risk assessment and management processes
2. **Protect**- outlines security controls for protecting data and information assets from access and physical control to maintaining protective technologies
3. **Detect**- it provides practices and guidelines for detecting anomalies in data security, implements systems and networks to unearth security breaches or incidences.
4. **Respond**- this function focuses more on risk management. It includes practices for planning responses to security events, mitigation procedures and measures for improving security resiliency.
5. **Recover**- the recover function includes plans, guidelines and measures an organization can follow to recover from damage incurred as a result of attacks

The NIST cyber security framework has been accredited as the most implemented framework (Ibrahim et al., 2018). This is because it guarantees security assurance as it addresses the main concepts or principles of cyber-security (ISACA, 2015). The framework is aligned to the three defence in depth theory concepts of information security which are prevention, detection and response (Yeboah, 2013).

	Risk Management Process	Integrated Program	External Participation
Tier 1: Partial	Organizational cybersecurity risk management practices are not formalized and risk is managed in an ad hoc and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements.	There is a limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. The organization may not have processes that enable cybersecurity information to be shared within the organization.	An organization may not have the processes in place to participate in coordination or collaboration with other entities
Tier 2: Risk-Informed	Risk management practices are approved by management but may not be established as organizational-wide policy.	There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established. Risk-informed, management-approved processes and procedures are defined and implemented and staff has adequate resources to perform their cybersecurity duties. Cybersecurity information is shared within the organization on an informal basis.	The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally
Tier 3: Risk-Informed and Repeatable	The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to a changing threat and technology landscape.	There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and validated. Consistent methods are in place to effectively respond to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.	The organization understands its dependencies and partners and receives information from these partners enabling collaboration and risk-based management decisions within the organization in response to events.
Tier 4: Adaptive	The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous cybersecurity activities. Through a process of continuous improvement, the organization actively adapts to a changing cybersecurity landscape and responds to emerging/evolving threats in a timely manner.	There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.	The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before an event occurs.

Figure 2. 4: NIST framework implementation tiers

Adapted from "A security review of local government using NIST CSF: A case study. *Journal of Supercomputing*" by Ibrahim, A., Valli, C., Mcateer, I., & Chaudhry, J. (2018) (p.3)

- **The framework profile**

The Framework Profiles aligns the framework Core Functions, Categories, and Subcategories with an organization's implementation plan. As the framework allows organizations to create a framework profile and the gap that exists between the current profiles (the current achievements of cyber security) and the target profile, (what is needed to achieve the anticipated cyber security risk management plans) it creates an opportunity to recognize where existing processes may be strengthened or where new processes can be implemented to realize the target profile. The drafters expressed that “successful implementation” of the Framework is based on an organization’s ability to achieve its Targeted Profiles. (Ibrahim et al., 2018)

- **Strengths**

One of the strengths of the framework lies in its ability to provide organizations with a method to assess and map its cyber security practices to those stipulated in the framework through implementation tiers (Ibrahim et al., 2018). The tiers enable auditors to measure how they manage cyber security risks taking into consideration the firms existing security practices (Krumay, Bernroider, & Walser, 2018). As it considers the business existing practices, the framework acts as an enhancement to the existing rather than a replacement making it flexible enough to adopt and implement (Ibrahim et al., 2018). By assessing its current security posture, the organization can determine which tier it belongs to. From a cyber-security perspective, larger firms are likely to be found in tier 3 and 4 whilst small firms are likely to be found in tier 1 and 2. According to Ibrahim et al. (2018), organizations are encouraged to progress to higher ties when a cost-benefit analysis indicates a feasible and cost-effective reduction of cyber security risk.

To add on to the aforementioned strengths of the framework, it provides a seven-step implementation process that is flexible to be used to develop new cyber security management practices or to complement the already existing ones (Krumay et al., 2018). Furthermore, the Framework can adapt to the changing environment as the cyber security landscape continues to evolve (Roberts, 2013). A roadmap that discusses the frameworks planned or targeted steps is issued before the release of the framework (Ibrahim et al., 2018).

In line with the above, the framework references globally recognized standards for cyber security meaning it can serve as an international framework that can fulfil the cyber security global duty. With implementation tiers and the frameworks profile, it gives organizations the privilege to adopt the framework in a manner that best fits the organization's requirements and current practices.

- **Limitations**

Contrary to the above, the framework provides a macro-overview of how organizations should deal with cyber security whilst leaving out implementation details relevant to each firm

(Ibrahim et al., 2018). Whilst the framework allows organizations to perform a security analysis, the depth of the analysis relies on organizational interpretation and preference. It does not propose control requirements. This probes for an assessment that can leave weaknesses undetected giving an organization or a firm a false sense of security (Alsinawi, 2018; ISACA, 2015). Similar to this, another scholar indicated that since the framework leaves organizations to decide which level or tier they belong to, it creates room for hackers as a result. The scholar further suggested that the framework should be enhanced to set firm standards for what tier level firms or organizations need to attain (Roberts, 2013).

2.8.3 ISO 27000 family of standards

The ISO 27000 standards are an information security standard that was developed by the International Organization for Standardization, and it provides guidelines for setting up management systems for information security through information security management systems family of standards (ISMS) (Drljača & Latinovic, 2017; Tarí, Molina-Azorín, & Heras, 2012). It includes ISO/IEC 27001, ISO/IEC 27002 and ISO 27005 standards which serve different purposes (Meriah, & Rabai, 2019; Devos, 2019). ISO/IEC 27001, ISO/IEC 27002 serve the purpose of reducing cyber security risks by providing guidelines or recommendations of all the requisite controls needed to implement and make use of ISMS (Tamimi, Aljohani, Alzahrani & Alharbi, 2019; del Castillo-Peces, Mercado-Idoeta, Prado-Roman, & del Castillo-Feito, 2018). According to Yeboah (2013), the ISO framework addresses compliance issues as it relates to organizational standards, regulatory/legal requirements, the organization's security policies and procedures and the documented information security management system. ISO standards are specific to information security, hence providing detailed guidelines on implementation, unlike COBIT (Asmah, 2019).

Be that as it may, as indicated by Barafort, Mesquida, and Mas, (2017), ISO standards still experience the ill effects of paucity and pundits are still an argument as to whether they constitute the complete sets of frameworks for auditing cyber security.

2.8.4. Trust Service Criteria

The TSC framework was developed by the American Institute Of Certified Public Accountants (AICPA) and it focuses on five main components namely security, availability, processing integrity, confidentiality and privacy (AICPA, 2017).

Components	Explanation
Security criteria	It is concerned with protecting an organization's information assets against hackers, and unauthorized users. It further ensures implemented systems integrity, privacy, availability and confidentiality are not compromised to an extent that an organization cannot meet its overall objectives. As aforementioned, the main objective of information security auditing is to test the effectiveness of implemented controls and systems against cyber threats (AICPA, 2017).
Availability	It addresses the availability of information and systems for use, including the accessibility of information for operation, maintenance and monitoring (AICPA, 2017).
Processing Integrity	integrity addresses an organization's systems main purpose. It puts in question whether implemented systems achieve the purpose that they were designed to fulfil in a right manner that is free from error, delay, omission or manipulation of information (AICPA, 2017).
Confidentiality	Alludes to necessities concerning the collection, use, retention, disclosure, and disposal of personal data. Confidential data may incorporate personal data as well as other data, for example, intellectual property (AICPA, 2017).
Privacy	Addresses how personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives. There is a thin line between privacy and confidentiality. Whilst confidentiality adheres to various types of sensitive information, privacy applies to personal information only (AICPA, 2017).

The framework provides principles that can be used to evaluate a company's information technology systems. It further provides best practices for system reliability (AICPA, 2020).

In adopting the framework, organizations may choose to adopt the whole framework or they may only select principles that are relevant to their business. This makes it flexible enough for organizations to map the framework with their business aims and goals. The "privilege" of choosing principles to adopt comes with the security principle as mandatory. This prompts organizations to address the security aspect of their organization. The framework is also simple enough thereby making it easier to adapt and implement. Whilst several credited frameworks are available, some of them are too complex and do not assess technology controls which is a strength of the TSC framework.

The sources of the TSC framework mainly emanate from its developers/publishers the American Institute of Certified Public Accountants (AICPA). There is no literature available that has critically evaluated the framework to date hence the actual utilization, relevance and effectiveness of the TSC framework is unclear.

Several of these frameworks have often failed to translate well into desired outcomes in auditing cyber security due to a lack of sufficient implementation guidance and unclear theoretical foundations. It can be noted that the frameworks in question have their strengths and weaknesses hence a comprehensive framework can be drawn from the fragments of the noted frameworks.

2.9 Summary of literature

The literature review has given an insight into the existing frameworks that are being used to audit cyber security in Organizations. Strengths and weaknesses of the frameworks have been noted. Literature has also analyzed the role of an auditor using underlying theories. Gaps in literature will now be presented.

2.10 Gaps in the literature

Literature fails to provide frameworks for auditing cyber security that were developed in Africa. Surveys and studies conducted on the development and adoption of the frameworks have mainly been from outside Africa. The NIST cyber security framework was developed in the United States, ISO standards originate from Switzerland, the COBIT framework was developed by the ISACA board which originated in and the Trust Service Criteria originate from America (Cockcroft, 2020; Goldman, 2005). To add on, scholarly reviews are scarce on the applicability of the frameworks to cyber security auditing, especially the TSC framework. Furthermore, the aforementioned cyber security frameworks have been found to be broad in use and expensive to adopt making it problematic to auditing cyber security. This means that 'only' large companies will be able to adopt them. Little information is available for the rules and regulations that govern banks adoption of cyber security frameworks. It remains vague whether financial institutions in South Africa are obliged to adopt cyber security frameworks or not.

Furthermore, literature that focuses on understanding the usability and adoption of the aforementioned frameworks in auditing cyber security and assessing the challenges faced in auditing cyber security is limited. This is due to the generally low level of theoretical and empirical grounding for cyber security auditing, especially within the African context.

2.11 Conceptual model

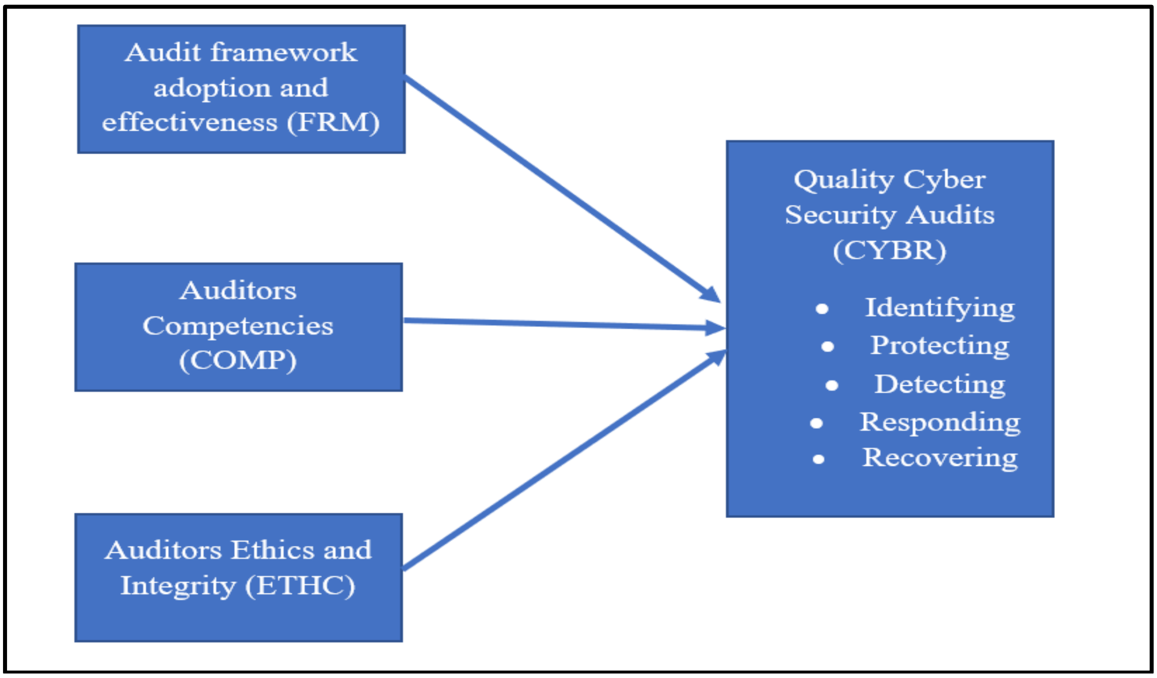

Figure 2. 5: A framework for enhancing the effectiveness of quality cyber security audits

The above model was developed from fragments of the aforementioned frameworks and theories.

2.12 Definition of Constructs and hypotheses

The definition of constructs from the above conceptual model is shown in the table below.

Table 2. 1: Definition of constructs

Construct	Definition	Source
Audit framework adoption and effectiveness	It serves as a structure with a set of guidelines, procedures and processes for performing an audit.	ISACA (2015) Ibrahim et al., (2018) Roberts (2013)
Auditors Competencies	These are the underlying characteristics of IT auditors, in terms of their knowledge and skills. IT auditors need these competencies to be able to perform quality audits.	Deloitte (2017) Osamah (2018) ISACA (2019)

Auditors Ethics and integrity	It entails to an auditors and organizations expected behavior and conduct in their line of work. It also includes an auditors ability to act ethically and with integrity in their line of work	Kshetri, (2019)
Quality Cyber security Audits	It is a validation to check if what the organization has said they have in their policy is in place and ensuring that there are controls and mechanisms put in place to enforce it. It also includes assessment of implemented systems to check their effectiveness, identify weaknesses and recommend solutions.	Deloitte (2017) ISACA (2015) ISACA (2010) Osamah et al., (2018)

2.13 Hypotheses

The following hypotheses were formulated based on the literature and from the conceptual model above.

Hypotheses 1: Cybersecurity Audit Framework effectiveness has a positive and significant effect on the quality of cybersecurity audits.

As new threats emerge due to innovations in technology, it is paramount to utilize an appropriate framework that will identify, protect, detect, respond and recover. This will allow the auditing team to timely manage risks thus enhancing the effectiveness of cyber security audits (Bumgarner & Vasarhelyi, 2015).

Hypotheses 2: Auditor's competencies have a positive and significant impact on the quality of cyber security audits.

Having 'inexperienced' IT auditors perform an audit may result in a poor audit which will give the organization a false sense of security (IIA, 2018). Research shows that it is necessary to have competent auditors who will be able to perform quality audits that will define an organizations security posture and identify weaknesses.

Hypotheses 3: An auditors' ethics and integrity have a positive and significant effect on the quality of the cybersecurity audits.

The goal of an audit is to protect information systems through identifying, protecting, detecting, responding, and recovering. For an audit to be effective and of quality, auditors have to ethically act and work with integrity without compromising their work.

Hypotheses 4: Alignment of an auditors' skills and competence, ethics and integrity coupled with an appropriate framework will result in enhanced cyber security audits that can identify, protect, detect, respond and recover.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

This chapter outlines the research methodology utilized in the conduct of this study. The goal of a research design and methodology is to provide a solution to the problem statement as defined above (Saunders, Lewis & Thornhill, 2019). It seeks to explain the underlying criterion for the chosen techniques and methods and how they apply to particular problems. Based on the problem statement, a framework that allows for the enhancement of quality and effective cyber security audits was developed. As such, the following study presents the philosophical considerations, research methods and guidelines in the context of this study.

3.2 Philosophical consideration

Research philosophy relates to the source, nature and development of knowledge (Saunders, Lewis & Thornhill, 2009). According to Saunders et al., (2009) Ontology and Epistemology are the two major philosophical positions as shall be explained below.

3.2.1 Ontology

Ontological stance refers to knowledge and the nature of being (Saunders et al., 2009). It also refers to the study of existence which is how we determine the existence of things. Yilmaz, (2013) states that there are 2 types of ontological stances which are objectivism and subjectivism. Objectivism and subjectivism have been portrayed as a continuum's opposites with changing philosophical positions adjusted between them. Objectivists believe that knowledge is readily available, it exists independently of social factors and can be collected objectively (Saunders, Lewis & Thornhill, 2019). On the contrary, subjectivists believe that knowledge is constructed from the views and actions of human beings (Holden & Lynch, 2004). Saunders et al., (2009) further posited that subjectivists maintain that reality does not exist outside oneself. To echo this, Saunders (2019) is of the notion that for the researcher to understand human actions, they need to explore the subjective meaning stirring the actions and this can be through observation.

This study seeks to define the factors that influence the effectiveness of quality audits. This will be done through examining existing frameworks, the role and effectiveness of audits in cyber security. This information exists within the cyber security professionals, financial institutions, and information technology auditors. As a result, this study will be using an objectivism approach which postulates that the knowledge of human beings and their values are objective, and knowledge exists and is there for use by the researcher (Goertzen, 2017; Saunders et al., 2009).

3.2.2 Epistemology

Epistemology is a theory of knowledge that seeks to give lucidity to the idea of how knowledge is acquired (Levers, 2013; Patten, & Newhart, 2017). It clarifies how knowledge is applied and why it has its existing features. Epistemology presumes that knowledge does exist, and it anticipates being utilized by researchers for objective measuring (Holden & Lynch, 2004). Although there other epistemological positions such as critical realism, this study will look at two main epistemological positions which are positivism and interpretivism (Saunders *et al.*, 2019). Interpretivists assume that access to reality is through social developments or constructions (Queirós, Faria, & Almeida, 2017).

The positivism stance entails that research is being carried out objectively without the interruption or involvement of the researcher (Saunders et al., 2009). It likewise advances that the circumstance a researcher intends on examining and observing can be separated into underlying elements (Saunders, 2019).

According to Creswell (2014), the critical realist or pragmatist paradigm exists to bridge the gap between interpretivists and positivists. Pragmatists relate to the use of mixed methods in research and advocate for truth and reality, that is what works as the truth with regards to research questions. According to Kankam, (2019) the pragmatist paradigm also relates to qualitative studies as it is more concerned with actual results rather than theoretical foundations.

This study adopts the positivist paradigm. According to Creswell, (2014) positivism relates to the objectivism stance and studies. This makes the positivist paradigm suitable for examining financial institutions cyber security posture including major drawbacks in existing frameworks. It is also suitable because it allows for observation and measurement of constructs in the conceptual model developed in the study.

3.3 Research method

Two research methods exist at the disposal of researchers. The two comprise of qualitative and quantitative research methods (Holden & Lynch, 2004). The qualitative approach is subjective and is expedient when an interpretivism paradigm is selected. It seeks to gain insights into a research problem (Saunders et al., 2019). The quantitative method is based on objectivism and the positivism paradigm. It is concerned with one of its objectives which is to produce accurate and reliable data that allow for statistical analysis (Saunders *et al*., 2009). This study adopts the quantitative research method to measure the variables developed in the conceptual model and to formulate a relationship between them (Saunders et al., 2019).

3.4 Research Purpose

Research purpose can be categorized as descriptive, exploratory and explanatory (Saunders et al., 2019). Saunders et al., (2009) further posit that, while descriptive research seeks to explain and provide descriptive information on a phenomena, exploratory research is characterized by its flexibility as it seeks to study a new phenomenon. The explanatory research purpose is grounded in theory and seeks to observe an existing phenomenon, obtain a better understanding of it and uses theories or hypotheses to explain forces that caused a phenomenon to occur. Explanatory research attempts to understand cause and effect through connecting ideas (Holden & Lynch, 2004).

This study is explanatory as a conceptual model was developed based on existing literature and theories. The study also uses hypothesis to better understand cause, effect and relationships between aspects.

3.5 Approach to theory development

There are two types of reasoning that exist, and these are deductive and inductive reasoning. Deductive reasoning refers to the concept of how one reaches a conclusion and how they believe their conclusion to be true (Saunders *et al.,* 2019). Deductive reasoning requires the researcher to start with general principles or premises, develop existing theory and test to logically formulate a conclusion (Creswell, 2014). Based on the logic of processes, deductive reasoning is meant to prove if the conclusion is true. On the contrary, inductive reasoning uses observation to formulate a conclusion. A theory is formulated after data collection and is based upon data collection results (Creswell, 2014; Saunders *et al*., 2019).

This study followed the deductive reasoning approach in that existing theories were used to explain underlying factors and a conceptual model was developed. This allowed a systematic drawing of valid conclusions based on testing of given hypotheses that have been derived from the conceptual model.

3.6 Research Strategy

The survey approach was selected as a research strategy for this study as it allows the quantitative type of data collection from the target population. The survey approach relates to deductive research and is most fitting for ‘what’ and ‘how’ research questions (Saunders et al., 2019). It is concerned with collecting and analyzing data without interrupting the respondents. Surveys mainly employ questionnaires as a data collection technique although it also uses observations and structured interviews. As such, this made the strategy suitable for this study as it follows the positivist stance. According to Saunders et al., (2009), the survey approach allows for an economical way of collecting data from large populations.

3.7 Research time frame

The research time frame can either be cross-sectional or longitudinal (Saunders et al., 2009). This research will use a Cross-sectional time frame because the data collection and research will happen only once for a limited period in time which is what defines the cross-sectional time frame. This research study is also cross-sectional due to the duration of the master’s program which is for 24 months. On the contrary, a longitudinal time frame allows for observations to be done over a long period hence will not be suitable for this study.

3.8 Data collection and process

This section presents the target population, data collection and analysis, sampling technique and how the research instrument for data collection was designed.

3.8.1 Target population and sample

Target population refers to an entire set of cases or of people from which the researcher intends to conduct research and draw conclusions from (Taherdoost, 2016). Due to limited time and resources, it is almost impossible for researchers to analyze the entire population so a sampling technique is applied which reduces the population and allows only a subset of the population to be analysed (Taherdoost, 2016).

The target population for this study is information technology auditors and cyber security professionals in South African financial institutions. Kshetri (2019) noted that the rate of cybercriminals was on the rise in emerging countries in Africa more than in any other area in the world and the financial sector is at high risk. Furthermore, according to the South African Banking Risk Information Centre, the Republic of South Africa loses around $157 annually to cyber-attacks. For this reason, South Africa was chosen since it belongs to the African continent and IT auditors and cyber security professionals were chosen as they constitute the auditing team. The target population was chosen because of the need for the study to be conducted in a different context and also because cyber-attacks were noted to be rampant in the African context. South Africa was hence chosen as it is in the African context. The researcher obtained a list of auditors and cyber security professionals from ISACA board (South African chapter) which is a professional board with whom IT auditors and cyber security professionals are registered. This provided reliable and complete information about the target population. The unit of analysis is the individual auditor and cyber security professionals who are working for financial institutions in South Africa.

3.8.2 Sampling technique

Sampling is the process of selecting a subset of the population to be observed. The study uses a purposive sampling method. Purposive sampling entails that the researcher will be collecting data from professionals who have the required knowledge and experience. Sample size refers to the actual number of participants included in a study (Saunders et al., 2009).

For statistical analysis, Saunders et al., (2009), is of the notion that a sample size of 30 or greater is adequate. However, the magnitude of sampling error can be diminished by increasing the sample size hence targeted number of participants for this study was 60 based on purposive sampling and also because there are greater sample size requirements in a survey-based study.

Table 3. 1: Population and sampling

Population	South African financial institutions
Unit of analysis	IT Auditors and cyber security professionals
Sampling technique	Purposive sampling
Sample size	60

3.8.3 Data collection method and analysis

There are three methods of data collection applicable to data collection namely interviews, questionnaires, and observation (Saunders *et al.,* 2019). Studies that mainly employ the survey strategy use a questionnaire as the method of collecting data. A questionnaire hence is suitable for this study. Questionnaires are ideal for this study as they yield data for a quantitative type of research (Van Schaik et al., 2017). The quantitative research data which was obtained in the study was derived from the questionnaire distributed to participants. Structured questionnaires were used in this study for data collection. The advantage of using questionnaires is that it is easy to administer to a large sample all at once which saves time. Participants indicated their profession, position in the organization, years of experience and age among other things. The questionnaire was structured in such a way that it provided a brief explanation of reasons for conducting the research and the importance of the respondent's input.

Scales

This section defines the different types of scales and identifies the scale that was used for this study.

Nominal and categorical scales: These are scales that appoint qualities to objects just to distinguish or arrange, not measure them. They are utilized where factors have unrelated alternatives, for example, gender. Its data cannot be estimated, however, it can be arranged or categorized (Mishra, Pandey, Singh, & Gupta, 2018).

Ordinal scales: it is a scale of measurement whereby variables have ordered categories (Younas, & Porr, 2022).

Binary scales: They are nominal scales that accept one of two possible values for example respondents answer 'yes' or 'no', 'true' or 'false' (Younas, & Porr, 2022).

Categorical scales: a sequence of numbers that identify items as belonging to mutually exclusive categories (Mishra et al., 2018).

Likert scales: measures ordinal data and respondents indicate the extent to which they agree or disagree with (Younas, & Porr, 2022).

For this study, a likert scale and a categorical scale was used. The research instrument design section which is attached as appendix A indicates how the questionnaire was designed.

3.8.4 Data analysis

For this study, data was captured, stored, cleaned, and standardized using Microsoft Excel. Data analysis was done using a software called Statistica. It was used to examine the hypothesis to the constructs formulated and to propagate the results. Data was tested for normality and reliability. Several methods exist for testing or for determining which construct has a normal distribution. The known methods for testing normal distribution are the histogram, the box plot, the Kolmogorov-Smirnov test, the Quantile vs Quantile plot which plots theoretical quantiles against the actual quantiles of the variable and the Shapiro-Wilkin test (Meeker & Escobar, 1998). Experts regard the Shapiro Wilk test as one of the most powerful tests when testing for a normal distribution. Shapiro Wilk test is a parametric test that makes some assumptions about the data whereas the KS test is a non-parametric test that does not make any assumptions about the data. If the P-Value of the Shapiro Wilk Test is larger than 0.05, we assume a normal distribution. If the P-Value of the Shapiro Wilk Test is smaller than 0.05, we do not assume a normal distribution (McDonald, 2013). The importance of testing for normality is to know where to use parametric and non-parametric tests appropriately.

To assess the quality of research, reliability and validity tests were done. Issues related to reliability include respondents' error and bias and to address this, questions in the questionnaire were clear to avoid ambiguity and misinterpretation. The technique that was used to test reliability is the Cronbach alpha reliability test. A reliability test measures the internal consistency of items measuring a construct (Meekar & Escobar, 1998). Cronbach's Alpha indicates the extent to which items measuring a construct are interrelated thus it can be used to measure the overall reliability (Ware & Gandeka, 1998). Cronbach's Alpha ranges between 0 and 1 with values closer to 1 indicating a higher consistency and values closer to 0 indicating a lower consistency. A threshold of 0.60 is the least reliable value, 0.70 is the acceptable value whilst 0.90 is deemed an excellent value of Cronbach's alpha (Lakens, 2016).

3.9 Research instrument design

A research instrument, in the form of a structured questionnaire, was developed and was administered to respondents. The research questions in the research instrument measure all the constructs in the conceptual model. With categorical data, data values cannot be measured numerically but can be classified into types according to the features that identify or describe the variable (Kothari, 2004). To design the research questionnaire, some relevant questions from recent studies and surveys were adopted as is and other questions were adapted, customized and contextualized to fit this particular study.

Section A of the questionnaire captures the demographic details of participants. Section B captures framework adoption and effectiveness. Section C measures an auditors competencies, Section D measures an auditors ethics and integrity and section E measures the quality of cyber security audits. The questionnaire is attached as appendix A and the questionnaire introductory letter is attached as appendix B. The table below provides a summary of the research design instrument, and it includes the constructs, source and data type. The questionnaire was pilot tested for validation before use.

Table 3. 2: Structure of the questionnaire

Construct	Source	Data type
Section A- Demographic data	Jamisson (2018)	Categorical
Section B- Audit framework adoption and effectiveness	ISACA (2015)	Likert
Section C- Auditors Competencies	ISACA (2019)	Likert
Section D- Auditors Ethics and integrity	Kshetri (2019)	Likert
Section E – Quality Cyber Security Audits	Deloitte (2017)	Likert

3.9.1 Resources and plan

This research was conducted in South Africa. The questionnaire was developed using a software called Qualtrics and a link to the questionnaire was shared to the respondents via email and LinkedIn which was cost-effective. Due to this, there were no financial resources needed during the data collection phase.

3.10 Ethical considerations

Ethical issues are of much concern when dealing with research that involves human participation (Joshi & Goyal, 2011). Research ethics relate to how researchers gain access to participants, collect, store analyze and interpret data in an ethical, moral and accountable manner (Saunders et al., 2019). One of the important aspects of ethical issues is that participants must contribute at their free will or voluntarily without any coercion and they can withdraw from the study at any time that they may want (Joshi & Goyal, 2011). This research used surveys for data collection and the University of Cape Town (UCT) has prescribed rules and standards on the ethical process of collecting data. The rules and standards include an ethics cover letter, participant Consent Form and a research application form. Ethical considerations that were made in this study included getting ethical clearance from the department, ensuring informed consent for participation in the study, confidentiality and anonymity, storage and analysis of data collection and publication of the results of the study.

Ethical Clearance Form: For this research, the researcher applied for ethical clearance from the University of Cape Town Ethics Committee before data collection and it was approved. The ethics clearance form is attached as appendix C.

Informed Consent: Consent for IT auditors and cyber security professionals to participate in the study was sought from ISACA board (South African chapter). To facilitate approval of access to auditors and cyber security professionals, an application to the ISACA board (SA chapter) was made which is part of the board requirements, ethics letterheads outlining the type of data to be collected and the purpose of the research was sent as part of the application. Consent forms included the purpose of the research and informed participants of their right/choice to participate willingly/freely or withdraw from the study at any point. It was communicated to participants that no harm would be done as a result of this study and that their anonymity was guaranteed. Data collection application to ISACA board is attached as appendix D and the approval is attached as appendix E.

Confidentiality and anonymity: To ensure privacy and confidentiality, the structured questionnaire for data collection did not require research participants to provide personal identifiable details.

Data Storage and Analysis: Data collected was securely stored in a password-protected personal computer and the data was backed up on a secure cloud account. Data was cleaned accordingly before the analysis stage.

Publication: Participants were informed that the results of the study will be published, and the researcher revealed her identity to the respondents.

3.11 Research design summary

Research Step	Study Selection
Philosophy	Ontology - objective Epistemology - positivism
Approach to theory	Deductive
Purpose	Explanatory
Methodological choice	Quantitative
Strategy	Survey Approach
Data collection	Primary data - questionnaire
Data analysis	Statistica
Timeframe	Cross sectional
Sample selection	Purposive

CHAPTER 4

DATA ANALYSIS, PRESENTATION AND DISCUSSION

4.1 Introduction

This chapter focuses on the analysis and presentation of the collected data. The preceding chapter discussed the methodology used to gather data, and how data was analyzed and processed into findings. This chapter focuses on the transformation of data into findings that answer the research questions, in line with the research objectives. After interpretation of results, the findings are discussed in relation to the reviewed literature to determine conflicts and concurrences between the findings of this study and the reviewed literature, which helps understand the extent to which this study contributes to closing the current research gap and solving the research problem.

4.2. Data cleaning

Data cleaning refers to the modification, correction and or deletion of identified errors and inconsistencies in a data set (Karam & Ralston, 2016). Errors in data may be due to incorrect entry of the data or corruption. Literature has credited data cleaning as emblematic of data quality issues (Karam & Ralston, 2016). Inconsistencies and errors in data reduces the quality of the analysis results hence data cleaning is vital (Broeck, Cunningham, Eeckels, & Herbst, 2005). Data cleaning for this study was done using Microsoft excel. No outliers (extreme data values) were identified in the data. Some of the data however had missing values. Broeck et.,al (2005) suggest certain measures in dealing with missing information. These include investigating the total amount of missing data, investigating the pattern and impact of missing data and identifying appropriate techniques to deal with missing data. Rule of thumb was used to deal with missing data. Rule of thumb states that if less than 15% of variables is missing, data may be deleted but data may be treated where 20-30% is missing. Responses with missing data were deleted hence from 55 responses, only 50 were left to be analysed.

4.3 Response rate

60 experts were considered adequate to participate in this study. Out of the 60 invited participants, 55 accepted the invitation and consented to participate in the study. The local chapter of ISACA approved the use of its members for the study. Total respondents from ISACA local chapter were 55 and after data cleaning, 50 were left to be analyzed. The survey ensured the anonymity of the respondents which enhanced the instrument's reliability as the respondents completed the survey without any face-to-face interaction thereby eliminating any form of influence or bias.

Saunders et al. (2019), regard response rate to be the percentage of completed instruments relative to the total number of instruments distributed. The response rate on the questionnaire used is presented in Table 4.1.

Table 4. 1: Response rate

Questionnaires distributed	Successful	Response rate
60	50	**85.71%**

The response rate on the questionnaire was therefore 85.71% as indicated in Table 4.1. The remaining 14.21% of the targeted participants could not participate successfully in the data collection process due to reasons like reluctance, being too busy and being absent during data collection period. According to Vaske, Beaman, and Sponarski, (2017), a response rate that exceeds 70% is reliable. As a result, the response rate for this study was considered reliable to validate the generalizability of the results.

4.4 Pilot Study

A preliminary version of the questionnaire for this study was distributed amongst four people, (two IT auditors and two senior lecturers from the University of Western Cape). It was found that the questionnaire was too long and daunting to answer, some questions were vague and not relevant. Valuable feedback was attained from the pilot study and recommendations from the professional and academic experts was integrated into the questionnaire which helped to validate the questionnaire. With the consultation of the supervisor, the questionnaire was restructured and modified, some questions were changed, and a Likert scale was used. This resulted in a more relevant, accurate and reliable questionnaire.

Qualtrics was used to distribute the survey. Respondents` confidentiality and anonymity were emphasized on the cover page of the questionnaire and an estimated completion time of the survey was suggested based on the conducted pilot study. The researcher briefly introduced herself to the respondents and provided her contact details. Moreover, to add prominence, credibility and to help with recognition, the University of Cape Town ideogram was on the cover letter of the research instrument.

4.5 Reliability statistics

Bryk and Raudenbush, (1992), regards reliability as the internal consistency of the instrument, which shows the degree to which an instrument can be used using different samples drawn from the same population, with similar findings being obtained in each case. To add on, another scholar is of the notion that a reliability test measures the internal consistency of items measuring a construct (Meekar & Escobar, 1998). A commonly used test for internal consistency of responses is Cronbach's Alpha. Cronbach's Alpha indicates the extent to which items measuring a construct are interrelated thus it can be used to measure the overall reliability (Ware & Gandeka, 1998). Cronbach's Alpha ranges between 0 and 1 with values closer to 1 indicating a higher consistency and values closer to 0 indicating a lower consistency. A threshold of 0.60 is the least reliable value, 0.70 is the acceptable value whilst 0.90 is deemed an excellent value of Cronbach's alpha (Lakens, 2016). Taber (2018) and Goodnight (1980) also highlighted that a Cronbach's Alpha between 0.6 and 0.9 shows high reliability of the instrument and results.

The results on the reliability of the questionnaire on each construct were presented in this section.

Table 4. 2: Reliability statistics for the Audit Framework construct

Reliability Statistics

Cronbach's Alpha	N of Items
.879	21

The Cronbach's Alpha in Table 4.2 is 0.879, which shows that the questionnaire was highly reliable as far as the audit framework construct or variable (made up of 21 items or questions) is concerned, and hence the results were highly dependable and generalizable on the study population.

Table 4. 3: Reliability statistics for the competencies of auditors construct

Reliability Statistics

Cronbach's Alpha	N of Items
.823	9

The Cronbach's Alpha in Table 4.3 is 0.823, which shows that the questionnaire, was highly reliable in terms of the competence construct (which was made up of 9 items or questions), hence the results were highly dependable and generalizable on the study population.

Table 4. 4: Reliability statistics of an auditors ethics and integrity construct

Reliability Statistics

Cronbach's Alpha	N of Items
.849	5

The Cronbach's Alpha in Table 4.4 is 0.849, which shows that the questionnaire was highly reliable in terms of the ethics construct or variable, and hence the results were highly dependable and generalizable on the study population.

Table 4. 5: Reliability of quality cyber security audits construct

Reliability Statistics

Cronbach's Alpha	N of Items
.721	6

The Cronbach's Alpha in Table 4.5 is 0.721, which shows that the questionnaire was highly reliable in terms of the cyber security audit quality construct or variable.

4.6 Demographics and background information of participants

The descriptive statistics of the demographics of respondents are presented in this section, starting with the age range.

4.6.1 Age range of participants

The results on the participants' age range are presented in Table 4.6.

Table 4. 6: Age of respondents

Age range

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	20 - 30 years	12	24.0	24.0	24.0
	30 - 40 years	35	70.0	70.0	94.0
	40 - 50 years	3	6.0	6.0	100.0
	Total	50	100.0	100.0	

Source: Primary data (2021)

The results in Table 4.7 indicate that the modal age group of participants is 30 – 40 years, which constitutes 70% of the respondents, followed by the 20-30 years category with 24% of the respondents, with the least populous range being the 40-50 years which is constituted by 6% of the participants. Therefore, the median age group of the participants is below 35 years, and the skewness of the age variable is negative, implying that younger ages were more dominant than older ages. This was quite important to the study as it gave a good picture that there were fresher minds than older ones. Also, all age groups were represented, hence the effects of age differences on results validity were minimized or somehow neutralized.

4.6.2 Levels of education

The results on participants' level of education are presented in Table 4.8.

Table 4. 7: Participants' highest level of education

Highest level of education

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Diploma	1	2.0	2.0	2.0
	Bachelor's degree	19	38.0	38.0	40.0
	Master's degree	23	46.0	46.0	86.0
	Doctoral degree	6	12.0	12.0	98.0
	Other	1	2.0	2.0	100.0
	Total	50	100.0	100.0	

Source: Primary data (2021)

The results in Table 4.8 indicate that the majority of the participants held Masters' degrees (46%), followed by 38% with bachelor's degrees. Diploma qualification was held by the least number of participants (2%), and the other 2% also held other qualifications besides degrees.

The results indicate that at least 98% of the participants had tertiary education, which implied that the participants were generally highly educated enough to understand concepts and questions on the questionnaire and to give highly valid responses based on at least theoretical knowledge acquired from learning institutions. Also, most of the participants are highly educated because of the requirements needed for one to be an IT auditor and/or a cyber security professional.

4.6.3 Certifications held

Table 4.9 presents results on the certifications acquired by the participants.

Table 4. 8: Certifications

Certifications

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	CISA	27	54.0	54.0	54.0
	CIA	2	4.0	4.0	58.0
	CISSP	7	14.0	14.0	72.0
	Other	14	28.0	28.0	100.0
	Total	50	100.0	100.0	

Source: Primary data (2021)

The results in Table 4.9 indicate that the majority of the participants held CISA (54%), followed by others (28%), with the least being the CIA (4%). The results indicate that there were wide variations in certifications, which was regarded by the researcher to have a positive effect on the study as variations in certifications would result in variations in experiences, opinions and so forth, which would render the results more representative of the entire population. 68% constituted IT auditors and cyber security professionals which was the target population of the researcher.

4.6.4 Job title

The results on participants’ job titles are presented in Table 4.10.

Table 4. 9: Job title

Job title

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	IT Auditor	36	72.0	72.0	72.0
	Financial Auditor	1	2.0	2.0	74.0
	Cyber security professional	2	4.0	4.0	78.0
	Other	11	22.0	22.0	100.0
	Total	50	100.0	100.0	

Source: Primary data (2021)

The results in Table 4.10 indicate that the majority of the participants were IT auditors (72%), followed by those with other titles namely IS specialists, IS consultant, IT risk and compliance manager and an IT technician, with the least being financial auditors who constituted 2% of the participants. The results indicate that all the job titles that the researcher regarded as more appropriate for the study were represented, which helped collect views, opinions, facts and experiences from all job titles deemed more appropriate for the study, thereby improving the representativeness of the results.

4.6.5 Job industry

Table 4.11 presents results on the job industry of the respondents.

Table 4. 10: Job industry

Job Industry

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Financial Sector	20	40.0	40.0	40.0
	Health Sector	5	10.0	10.0	50.0
	IT Sector	2	4.0	4.0	54.0
	Law Sector	3	6.0	6.0	60.0
	Other	20	40.0	40.0	100.0
	Total	50	100.0	100.0	

Source: Primary data (2021)

From the results, the majority of the participants were from the financial services sector (40%), followed by the totality of other sectors in which the respondents had to type the other sectors that were unspecified in the questionnaire. The other sectors which constituted 40% included people who work in audit firms, the public sector and chemical engineering sector sectors, with the least being the IT sector which constituted 4% of the participants. Different sectors were represented in the study, therefore this helped validate the generalizability of results on the entire population.

4.6.6 Years in the profession

Table 4.12 shows the results on the level of professional experience of the participants

Table 4. 11: Years in profession

Years in profession

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-3	3	6.0	6.0	6.0
	3-5	15	30.0	30.0	36.0
	5-7	17	34.0	34.0	70.0
	7-10	15	30.0	30.0	100.0
	Total	50	100.0	100.0	

Source: Primary data (2021)

The results in Table 4.12 show that the majority of the participants had 5-7 years of experience in their professions (34%), followed equally by 3-5 years and 7-10 years (with each constituting 30%). The smallest category is the 1-3 years with 6% of the respondents. The results indicate that 64% of the participants had at least 5 years of experience in their professions, which period the researcher considered long enough for one to have experienced most if not all of the aspects related to their profession, cyber security (practices and audits) in this case. This would enable them to give responses that are based mainly on experiences rather than perceptions and opinions. Factual or objective data was more necessary in this study given that the study was a quantitative, hence a high level of working experience of the respondents would help improve the validity and generalisability of results.

4.6.7 Location of business

Table 4.13 presents results on the location of participants' businesses.

Table 4. 12: Business location

Location

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Gauteng	6	12.0	12.0	12.0
	Western Cape	3	6.0	6.0	18.0
	Eastern Cape	1	2.0	2.0	20.0
	Free State	39	78.0	78.0	98.0
	Northern Cape	1	2.0	2.0	100.0
	Total	50	100.0	100.0	

Source: Primary data (2021)

The results indicate that the majority of the participants were from Free State (78%), followed by Gauteng (12%), with the least being Eastern Cape (2%). Although there seems to be a disproportionally larger number of participants from Free State province than all the rest, the participants were from a wide range of provinces, which the researcher regarded as highly useful in neutralizing effects of studying only from one area/province. The data was therefore collected from quite a huge number of provinces in South Africa, which the researcher regarded as important in improving the generalizability of results across the entire country.

4.7 Cyber security Frameworks

The first objective of the study sought to analyze the current frameworks used for cyber security auditing in financial institutions. Table 4.14 presents the various audit frameworks that have been adopted by the organizations under study, and their evaluations are presented in the succeeding section.

Table 4. 13: Cyber security audit frameworks

Which of these frameworks does your audit function frequently use for cyber security audits?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	COBIT	12	24.0	24.0	24.0
	NIST Cyber security Framework	23	46.0	46.0	70.0
	ISO 27001:2013 Standards	15	30.0	30.0	100.0
	Total	50	100.0	100.0	

Source: Primary data (2021)

The results in Table 4.14 indicate that the NIST Cyber Security Framework is used most by the organizations under study (46%), followed by the ISO 27001:2013 Standards (30%) and the least adopted is the COBIT (24%). Furthermore, the results indicate that none of the company's are using the TSC. Literature on the implementation of the TSC framework was limited and this tallys' with the results of this study. There are no other cyber security frameworks that have been adopted apart from these three. The result indicate that at least every framework understudy has been adopted by some institutions except the TSC framework. These results agree with prior surveys conducted including literature in which various authors had accredited the NIST cybersecurity framework as the widely implemented framework. According to a study conducted by ISACA and PROTIVITI, (2019), NIST was the widely implemented followed by COBIT and lastly ISO standards. For this study, the ISO came second and the COBIT came last. However, it is important to note that the studies in literature were dominantly conducted in other continents outside of Africa which could explain the difference.

4.8 Descriptive of study variables

This section analyses the descriptive of the study variables, in line with the study objectives. The variables of interest were the Audit Framework adoption and effectiveness (FRM), Auditors competencies (COMP), Auditors ethics and integrity (ETHC), and quality cyber security audits in identifying, detecting, protecting, responding and recovering to cyber security risks (CYBR), which is the dependent variable. The first objective of the study sought to evaluate the current frameworks used for cyber security auditing in financial institutions, which was done through analyzing the descriptive statistics of the variables.

The study adopted the following Likert scale: 1 = Not sure; 2 = Not effective; 3= Somehow effective, 4 = Effective; 5 = Very effective. As a result, mean values closer to 1 (less than 1.50) indicate that the respondents are generally not sure about the status of the variable. Mean values closer to 2 (from 1.50 to less than 2.50) indicate that the respondents have generally rated a variable to be ineffective. Mean values closer to 3 (from 2.50 to less than 3.50) indicate that the respondents have generally rated a variable to be somehow effective. Mean values closer to 4 (from 3.50 to less than 4.50) indicate that the respondents have generally rated a variable to be effective. Mean values closer to 5 (at least 4.50) indicate that the respondents have generally rated a variable to be very effective. Results on the descriptive statistics of the study variables are presented in Table 4.15.

Table 4. 14: Descriptive statistics

Descriptive Statistics

	N	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
FRM	50	3.8000	.41601	.411	.337	.544	.662
COMP	50	3.4164	.44564	-.506	.337	1.273	.662
ETHC	50	3.7280	.44218	-.714	.337	1.167	.662
CYBR	50	3.7800	.50669	-1.334	.337	2.422	.662
Valid N (listwise)	50						

Source: Primary data (2021)

The results in Table 4.15 indicate that the mean response on the evaluation of the current audit frameworks (FRM) was 3.8000, which, according to the scale used, implies that the respondents generally rated the current audit framework adopted as effective in improving the quality and effectiveness of cyber security audits, such as in assessing vulnerabilities. The standard deviation of 0.41601 indicates that there was high consistency of the responses, hence the mean is highly reliable as a measure of the general position taken by every respondent. This result seems to conflict in terms of magnitude but not the direction with the claims by scholars like Jreissat et al., (2018) and Osamah et al., (2018) who noted that adoption of cyber security audit guidelines or frameworks helps improve the quality of cyber security audit for an organization very effectively.

Furthermore, the mean response on the competencies of auditors was 3.4164, with a standard deviation of 0.44564. The results indicate that the respondents are generally convinced that the competencies and skills possessed by an auditor are somehow effective in improving the quality of cyber security audit results. The small standard deviation implies less variability of actual responses, hence the mean is reliable. The results show that respondents regard the current competencies of auditors as somehow effective in improving the quality of cyber security audits.

Apart from that, the results indicate that a mean response with a weight of 3.7280 and a standard deviation of 0.44218 was obtained on an auditors ethics and integrity when conducting cyber-security audits. This result indicates that the respondent regards this variable as effective in cyber security quality improvement. The standard deviation is small, showing less dispersion of actual responses around the mean, implying high mean reliability. The mean value indicates that the respondents generally confirm the ethicality of cyber-security auditors as far as cyber-security audits are concerned.

In addition, the results show that a mean of 3.7800 and a standard deviation of 0.50669 was obtained on the cyber-security audit effectiveness variable. The standard deviation shows high consistency of actual responses. The mean value which is closer to 4 shows that the respondents have generally rated the variable as effective. This implies that currently, cyber security professionals generally regard the quality of cyber security as effective in meeting audit expectations. The result indicates that the respondents generally view the current quality of cyber security as of average nature in meeting the expectations of the audit, but not very exceptional.

4.9 Normality Tests

The study had to perform a correlation and regression analysis and hypothesis testing in line with the objectives of the study, and to determine whether to use parametric or non-parametric tests, normality tests had to be performed to determine the distribution of the data. Several methods exist for testing or for determining which construct has a normal distribution. The known methods for testing normal distribution are the histogram, the box plot, the Kolmogorov-Smirnov test, the Quantile vs Quantile plot which plots theoretical quantiles against the actual quantiles of the variable and the Shapiro-Wilkin test (Meeker & Escobar, 1998). Experts regard the Shapiro Wilk test as one of the most powerful test when testing for a normal distribution. Shapiro Wilk test is a parametric test which makes some assumption about the data. If the P-Value of the Shapiro Wilk Test is larger than 0.05, we assume a normal distribution. If the P-Value of the Shapiro Wilk Test is smaller than 0.05, we do not assume a normal distribution (McDonald, 2013).

The study used Shapiro Wilk tests, using a 5% level of significance. According to Leavy (2019) and Lakens (2013), where the p-value is at most 5% (the level of significance), then the variable is not normally distributed. Table 4.16 presents the results.

Table 4. 15: Normality tests

Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	Df	Sig.	Statistic	df	Sig.
FRM	.111	50	.168	.947	50	.026
COMP	.086	50	.200*	.986	50	.814
ETHC	.140	50	.016	.963	50	.120
CYBR	.123	50	.056	.966	50	.162

a. Lilliefors Significance Correction

*. This is a lower bound of the true significance.

Source: Primary data (2021)

The results in Table 4.16 indicate that the Competence variable, the Ethics variable and the Cyber security audit variable have significance values that exceed 5% (0.814, 0.120 and 0.162 respectively), which means that they are the only variables that are normally distributed. Only the FRM variable has a significant value that is at most 5%, which implies that it is not normally distributed. Since the majority of the variables are normally distributed, the study adopted Pearson's Correlation which is parametric as opposed to the non-parametric Spearman's correlation.

4.10 Correlation Analysis

The results of the correlational analysis between the variables under study are presented in Table 4.17. Pearson's correlation was adopted since half of the variables were normally distributed. Further, the CYBR (quality cyber security audits)variable was the dependent variable, and all the other factors were the independent variables hence only the correlation between

CYBR and other variables were considered useful in this study. The correlation between the independent variables, which may indicate multicollinearity, was not regarded as important to this study.

Table 4. 16: Correlations

Correlations

		CYBR	FRM	COMP	ETHC
CYBR	Pearson Correlation	1	.349*	.413**	.839**
	Sig. (2-tailed)		.013	.003	.000
	N	50	50	50	50
FRM	Pearson Correlation	.349*	1	.187	.346*
	Sig. (2-tailed)	.013		.194	.014
	N	50	50	50	50
COMP	Pearson Correlation	.413**	.187	1	.410**
	Sig. (2-tailed)	.003	.194		.003
	N	50	50	50	50
ETHC	Pearson Correlation	.839**	.346*	.410**	1
	Sig. (2-tailed)	.000	.014	.003	
	N	50	50	50	50

*. Correlation is significant at the 0.05 level (2-tailed).

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

Source: Primary data (2021)

The results in Table 4.17 indicate that there is a moderate positive and significant correlation between the quality of cyber-security audits and the audit framework adopted (r = 0.349; p = 0.013). This implies that the adoption of an audit framework is moderately associated with an improvement in audit quality, and there is sufficient statistical evidence for that nature of association.

Furthermore, the results indicate that a moderate positive and insignificant association exists between the auditor competencies and the quality of cyber security audits (r = 0.413; p = 0.003). This means that as the competencies and skills of cyber security audit personnel improve, this results in somewhat improved audit quality, and there is sufficient statistical evidence to support this association.

In addition, the results in Table 4.17 indicate that there is a strong positive and significant correlation between the ethicality of auditors and the quality of cyber security audits (r = 0.839; p = 0.000). This implies that as the ethicality of auditors improves, the audit quality strongly improves in response, and we are sufficiently confident about such a correlation.

4.11 Linear regression analysis of cyber security audit quality against each independent variable

In this section, the dependent variable, quality cyber security audits, was regressed against each independent variable as broken down into subsections. The results were also the basis of acceptance or rejection of the hypothesis as stated in the second chapter of the study.

4.11.1 Framework adoption against cyber security audit quality

Table 4.18 presents results on the regression results on the relationship between the adoption of a cyber-security framework and the audit quality.

Table 4. 17: Model Summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.349[a]	.121	.103	.47984

a. Predictors: (Constant), FRM

The results in Table 4.18 indicate that there is a moderate positive correlation between the quality of cyber-security audits and the adoption and effectiveness of the cyber security audit framework (r = 0.349). The adjusted r-square is 0.103, which implies that cyber security audit framework adoption explains up to 10.3% of the cyber security audit quality, which is a low explanation as excluded variables explain up to 89.7% of changes in audit quality.

Table 4. 18: ANOVA

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1.528	1	1.528	6.638	.013[a]
	Residual	11.052	48	.230		
	Total	12.580	49			

a. Predictors: (Constant), FRM

b. Dependent Variable: CYBR

The results in Table 4.18 indicate that the F-value is positive 6.638, and is significant (p = 0.013), showing that the model is quite fit to explain the dependent variable.

Table 4. 19: Regression coefficients

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.167	.630		3.440	.001
	FRM	.425	.165	.349	2.576	.013

a. Dependent Variable: CYBR

The results in Table 4.19 indicate that the constant is 2.167 and is significant (p = 0.001), whilst the beta value is positive 0.349, which shows that the cyber security audit framework adoption has a positive impact on quality cyber security audits, and the impact is significant at the 0.05 level (p = 0.013). This implies that as the organisation intensifies compliance with audit framework guidelines, the cyber security audit quality also improves, and we are sufficiently confident that such a relationship exists. Hypothesis 1 of the study stated that: Cyber security audit framework adoption and effectiveness has a positive and significant impact on the quality of cyber security audits. This has led to the acceptance of the stated hypothesis that cyber security audit framework adoption and effectiveness has a significant impact on the results quality of the audit. The results are in line with the findings of Jreissat et al. (2018); Osamah et al. (2018), Kshetri, (2019), Drljača and Latinovic (2017), Yeboah (2013), Ibrahim et al., (2018) and Roberts (2013) who determined that a positive and significant relationship exists between cyber security audit framework adoption and quality of audits.

4.11.2 Competencies of auditors against quality cyber security audits

The regression results on the relationship between an auditors competencies and audit quality are presented in this section.

Table 4. 20: Model Summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.413[a]	.171	.153	.46622

a. Predictors: (Constant), COMP

The results in Table 4.20 indicate that there is a moderate positive correlation between the quality of cyber-security audits and an auditors competencies (r = 0.413). The adjusted r-square is 0.153, which implies that the competencies of auditors explain up to 15.3% of the changes in quality cyber security audits, which is a low explanation since the excluded variables explain up to 84.7% of changes in audit quality.

Table 4. 21: ANOVA

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2.147	1	2.147	9.876	.003[a]
	Residual	10.433	48	.217		
	Total	12.580	49			

a. Predictors: (Constant), COMP

b. Dependent Variable: CYBR

The results in Table 4.21 indicate that the F-value is positive 9.876, and is significant (p = 0.003), showing that the model is quite fit to explain the dependent variable.

Table 4. 22: Regression coefficients

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.175	.515		4.225	.000
	COMP	.470	.149	.413	3.143	.003

a. Dependent Variable: CYBR

The results in Table 4.22 indicate that the constant is 2.175 and is significant (p = 0.000), whilst the beta value is positive 0.413, which shows that the competencies of auditors have a positive impact on quality cyber security audits, and the impact is significant at the 0.05 level (p = 0.003). This implies that as the competence and skills of audit professionals improve, the cyber security audit quality also improves, and we are sufficiently confident that such a relationship exists. Hypothesis 2 stated that: An auditors' competencies have a significant impact on the quality of cyber security audits. Based on the results, the null hypothesis was rejected. The study determines that auditors' competencies have a significant impact on the quality of the audit. This result concurs with the findings of previous researchers like Deloitte (2017), Osamah (2018) and Isaca (2019) who determined that cyber security professionals' competencies have a positive and significant impact on the quality of cyber security audits.

4.11.3 Auditors Ethics and integrity of professionals against quality cyber security audit

The regression results on the relationship between an auditors ethics and integrity and quality cyber security audits are presented in this subsection.

Table 4. 23: Model Summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.839[a]	.703	.697	.27877

a. Predictors: (Constant), ETHC

The results in Table 4.23 indicate that there is a strong positive correlation between the quality of cyber-security audits and the ethicality of auditors (r = 0.839). The adjusted r-square is 0.697, which implies that the ethicality of auditors explain up to 69.7% of the changes in cyber security audit quality, which is a high explanation since the excluded variables explain only up to 30.3% of changes in audit quality.

Table 4. 24: ANOVA

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	8.850	1	8.850	113.875	.000[a]
	Residual	3.730	48	.078		
	Total	12.580	49			

a. Predictors: (Constant), ETHC

b. Dependent Variable: CYBR

The results in Table 4.24 indicate that the F-value is positive 113.875, and is significant (p = 0.000), showing that the model is quite fit to explain the dependent variable.

Table 4. 25: Regression coefficients

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	.197	.338		.583	.563
	ETHC	.961	.090	.839	10.671	.000

a. Dependent Variable: CYBR

The results in Table 4.25 indicate that the constant is 0.197, and is insignificant (p = 0.563), whilst the beta value is positive 0.839, which shows that the integrity and ethicality of auditors have a positive impact on cyber security audit quality, and the impact is significant at the 0.05 level (p = 0.000). This implies that as the ethicality of auditors improves, the cyber security audit quality also improves, and we are sufficiently confident that such a relationship exists. Hypothesis 3 of the study stated: An auditors ethics and integrity have a positive and significant effect on the quality of cyber security audits. This has led to the acceptance of the stated hypothesis that ethics have a significant impact on the results of the audit. The results are in line with the findings of Yeboah (2013), Ibrahim et al., (2018) and Roberts (2013) who determined that a positive and significant relationship exists between ethicality and quality of audits.

4.12 Regression model

Using only the variables with significant impact on the cyber security audit quality, the regression model is presented as follows.

CYBR = 0.010 + 0.349FRM + 0.413COMP + 0.839ETHC + e

Where CYBR = Cyber security audit quality

FRM = Audit framework adoption

COMP = Competences and skills of audit professionals

ETHC = Ethicality and Integrity of audit professionals

e = error term

4.13 Multi-regression analysis

The multi-regression analysis of the linear relationship between the study variables

Table 4.27 shows the multi-regression model summary.

Table 4. 26: Model summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.844[a]	.713	.694	.28033

a. Predictors: (Constant), ETHC, FRM, COMP

Source: Primary data (2022)

The results in Table 4.27 shows that the correlation coefficient is 0.844, which indicates that there is a very strong positive correlation between the independent variables and the dependent variable. As the ethicality, effectiveness and adoption of an audit framework and competencies of auditors improve, the quality of cyber security audits strongly improves as well. The adjusted r-square is 0.694, which implies that up to 69.4% changes in audit quality can be explained by the independent variables used. This implies that the model is a strong predictor of the independent variable because other independent variables not included in the model explain only up to 30.6% changes in the dependent variable.

Table 4. 27: Anova

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	8.965	3	2.988	38.026	.000[a]
	Residual	3.615	46	.079		
	Total	12.580	49			

a. Predictors: (Constant), ETHC, FRM, COMP

b. Dependent Variable: CYBR

Source: Primary data (2022)

The results in Table 4.28 indicate that the F-value is positive 38.026 and is significant (p = 0.000). This implies that the model is fit to explain the dependent variable as the sample variables are independent.

Table 4. 28: Regression coefficients

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	-.169	.464		-.365	.717		
	FRM	.076	.103	.062	.736	.466	.878	1.139
	COMP	.091	.099	.080	.922	.361	.830	1.205
	ETHC	.899	.104	.784	8.634	.000	.757	1.321

a. Dependent Variable: CYBR

Source: Primary data (2022)

The results in Table 4.29 indicate that the constant is -0.169, implying that other variables not included in the study have a combined negative effect on cyber security audit quality, but this relationship is not significant (p = 0.717), implying that we have no sufficient evidence for the existence of such a relationship. B1 coefficient is 0.062, which shows that adoption of a framework and its guidelines has a positive impact on the quality of cyber security audit, but then we have no sufficient evidence to support the existence of the relationship ($p = 0.466$). Further, the results prove that B2 = 0.080, which implies that the competencies of auditors have a positive impact on cyber security audit quality, but the impact is not significant ($p = 0.361$). Moreover, the results indicate that B3 = 0.784, which implies that the ethicality and integrity of audit professionals have a positive impact on quality cyber security audits, and there is sufficient evidence to support the existence of the relationship ($p = 0.000$). From the results, one can note that an auditors' ethicality and integrity, competencies, framework effectiveness and adoption, in that descending order, have positive impacts on quality cyber security audits, and their combined effect, if aligned, explains up to 69.4% changes in audit quality. In terms of multicollinearity, the results show that the VIF values are all less than 10 and the tolerance values are all above 0.1, which means that there is no problem of multicollinearity among the dependent variables.

4.14 Conclusion

The chapter gave an analysis, presentation, interpretation and discussion of the findings. Statistica was used for data analysis, presentation of results was in form of tables, as frequencies and descriptives. Normality tests done showed that most of the variables were normally distributed, which led to the adoption of parametric tests like Pearson's correlation. Correlation and regression analysis were performed, where it was determined that, currently, the ethicality and integrity of auditors has the greatest effect on quality cyber security audits. The discussion of the results was done in line with the reviewed literature to determine where and how the results of this study either conflicted or concurred with the findings and claims of other scholars as reviewed in the second chapter of this research study. The next chapter focused on the summary, conclusions and recommendations of the study.

CHAPTER 5

SUMMARY, CONCLUSION AND RECOMMENDATIONS

The preceding chapter concentrated on the analysis of data into findings. This fifth and final chapter of the study presents the summary of the major findings of this research. Thereafter, the chapter concludes on the research questions and objectives as obtained from the findings of the study. Subsequently, recommendations are given based mainly on the results and the reviewed literature. Further, the chapter points to areas for further study in a quest to further close the research gap.

5.1 Introduction

The response rate, reliability, demographics and background information of the respondents were all appropriate in terms of sample representativeness. After analysing the collected data, the following findings were obtained under each indicated research objective.

5.2 Summary of findings

- Results in this study showed that aligning an auditor’s ethics and integrity, skills and implementing an effective framework will result in effective cyber security audits that will enhance the protection of information systems.
- Secondly, it was found that the NIST framework is widely implemented in South African financial institutions, followed by the ISO standards and lastly the COBIT framework.
- None of the organizations have adopted the TSC framework.

5.3 Research objectives and findings

The first objective of the study was to evaluate the current frameworks used for cyber security auditing in financial institutions. The study established that there is a moderate positive and significant correlation between the quality of cyber-security audits and the audit framework adopted ($r = 0.349$; $p = 0.013$). The study also established that the NIST Cyber Security Framework is used most by the financial institutions under study (46%), followed by the ISO 27001:2013 Standards (30%) and the least adopted is the COBIT (24%). There are no other cyber security frameworks that have been adopted apart from these three. It is also important to note that scholars have done little work on the TSC framework and respondents of this study also indicated that none of their organizations had adopted the TSC framework. This could be as a result of how the framework is general and does not focus on any particular component of IT. Results of this study indicated that the COBIT framework is more aligned to IT governance hence its effectiveness to auditing cybersecurity has loopholes. ISO standards were found to be more aligned to compliance of organizations to regulatory laws and policies during the audit process. Despite its loopholes, the NIST framework was found to be more aligned to cyber security making it the most effective in auditing. This was found to be consistent with literature which accredits the NIST framework as the widely adopted and effective (Deloitte, 2017). Overally, results indicate that despite their weaknesses, the current frameworks are effective in auditing cyber security and enhancing it and their inefficiencies have been in cooperated in the model developed.

The second objective was to analyse the current cyber security audit processes and security posture of financial institutions. Although most cases of cyber-attacks are left unreported, recent studies have shown an increase in cyber-attacks on financial institutions (Kshetri, 2019). As technology continues to advance, cyber threats also emerge showing that currently, financial institutions are vulnerable and at risk. To add on, an evaluation of literature has revealed cases whereby auditors where implicated in cases that led to an organization being vulnerable and at risk. This highlighted the importance of an auditor's role in the process of auditing particularly an auditor's skills, ethics and integrity. Through a mean of 3.7800, the results indicate that currently, cyber security professionals generally regard the quality of cyber security as effective in meeting audit expectations. In other words, the results alluded that the current cyber security audit quality is satisfactory but not exceptional.

The third objective was to determine the effectiveness of audits in reducing cyber threats. The study established that as auditors aim to detect, protect, and recover information systems, the effectiveness of audits is of paramount importance. Furthermore, the results indicate that a moderate positive and significant association exists between the auditor competencies and the quality of cyber security audits ($r = 0.413$; $p = 0.003$).

5.4 Conclusion

The study concludes that the NIST Cyber Security Framework is used most by the financial institutions under study followed by the ISO 27001:2013 Standards and the least adopted is the

COBIT. Nevertheless, the mere adoption of the current audit frameworks by the financial institutions has not satisfactorily resulted in improved quality of cyber security audits.

The study concludes that currently, the cyber security audit personnel are satisfactorily competent and possess the skills to use the frameworks and to conduct cyber security audits. Furthermore, the auditors generally view the current audit practices as not very satisfactory in improving cyber security. In terms of the ethicality and integrity auditors, the study concludes that an auditor’s ethics and integrity affect the outcome of the audit hence is very important. The study further concludes that the South African financial sector security posture is ‘weak’. Overall, the current cyber security audits are satisfactory but not exceptional.

The study concludes that the mere adoption of a cyber-security framework has a significant but small impact on the quality of cyber-security audits, although the two are positively correlated. In addition, the study concludes that there is statistical evidence that the ethicality of audit professionals has a positive impact on audit quality, therefore improving ethicality significantly improves the cyber security audit quality. The study thus concludes that aligning an auditors skills and competencies and implementing a relevant framework significantly improves the quality of cyber security audits.

5.5 Recommendations

Based on the results and reviewed literature, the study made the following recommendations;

The study determined a positive correlation between the use of audit frameworks and the quality of cyber security audits. However, only three frameworks have been adopted, with a bias towards the NIST framework. In that regard, the study recommends financial service institutions adopt a variety of audit frameworks and borrow recommendations from several frameworks including the model developed in this study to further improve audit quality.

In addition, the study established that a positive correlation exists between auditor skills and competencies and the quality of cyber security audits. However, the current competence levels of auditors are not exceptional. It is recommended that further training and screening be done by the financial service institutions to ensure that the auditors are highly skilled and competent. The current negative impact that competence has in audit quality as established by the study can be corrected through further training of audit staff.

Apart from that, the ethicality of auditors has a positive correlation with the quality of cyber security audits, but currently, the impact of ethicality is positive but insignificant. Literature has it that improved auditor ethicality significantly results in improved quality of cyber security audits. Unfortunately, the ethicality of auditors is just but of a fair nature. The recommendation given to financial service institutions here is that they need to instill ethical values and cultures in their audit staff and measures be put in place to deal with deviations from established ethical standards so that ethicality is improved and maintained.

Since cyber security is also a national concern, the study also recommends the government of South Africa at large to institute and enforce relevant laws that ensure the protection of information systems.

5.6 Areas for further study

The study focused on coming up with solutions for improving the quality of cyber security audits in financial service institutions in South Africa. Further studies are recommended to focus on the same topic but using a different industry altogether, such as in the manufacturing industry to determine the applicability of these results in other industries. There is also need to examine theoretical impact relevance in the African context. Further, the study used the questionnaire for data collection, and employed a quantitative methodology. Other studies may employ a different methodology, such as a mixed-method design whereby both quantitative and qualitative means of data collection and analysis can be employed, to enhance data triangulation.

REFERENCES

Adams, M. B. (1994). Agency theory and the internal audit. *Managerial auditing journal*.

Agyemang, J. K., & Badai, B. (2020). Corporate Failure in the Banking Sector: The Role of External Auditors. *Research Journal of Finance and Accounting, 11*(4). doi:10.7176/rjfa/11-4-03.

Aicpa. (2017). Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. Retrieved 11 April 2020, from https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices.

Alsinawi, B. (2018). Is the Nist Cyber security framework enough to protect your organization? Retrieved May 22, 2020, from https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2018/is-the-nist-cybersecurity-framework-enough-to-protect-your-organization.

Anomah, S., & Aduamoah, M. (2018). Proposed analytical procedure for the customization and implementation of cobit 5, an auditing tool: an action design research approach. EDPACS, 57(3), 15-34, doi: 10.1080/07366981.2018.1433933.

Asfaw, T. (2018). *Cyber Security Auditing Framework (CSAF) For Banking Sector in Ethiopia* (Doctoral dissertation, st. mary's University).

Asmah, A. E. (2019). *Towards the development of a COBIT 5-driven IT audit framework* (Doctoral dissertation, Faculty of Commerce).

Avgerou, C., & Walsham, G. (Eds.). (2017). *Information technology in context: Studies from the perspective of developing countries*. Routledge.

Axelsen, M., Green, P., & Ridley, G. (2017). Explaining the information systems auditor role in the public sector financial audit. *International Journal of Accounting Information Systems*, *24*, 15-31.

Barafort, B., Mesquida, A. L., & Mas, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. *Computer Standards & Interfaces*, *54*, 176-185.

Biddle, B. J. (1986). Recent developments in role theory. *Annual review of sociology*, *12*(1), 67-92.

Biddle, B. J. (2013). *Role theory: Expectations, identities, and behaviors*. Academic press.

Borghard, E. D. (2018). *Protecting financial institutions against cyber threats: A national security issue*. Carnegie Endowment for International Peace.

Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, *33*(4), 360-376.

Brackett, M. A., Elbertson, N. A., & Rivers, S. E. (2015). Applying theory to the development of approaches to SEL.

Broeck, J. V., Cunningham, S. A., Eeckels, R., & Herbst, K. (2005). Data Cleaning: Detecting, Diagnosing, and Editing Data Abnormalities. *PLoS Medicine, 2*(10). doi:10.1371/journal.pmed.0020267.

Bryk, A. S., & Raudenbush, S. W. (1992). *Hierarchical linear models: Applications and data analysis methods*. Sage Publications, Inc.

Bumgarner, N., & Vasarhelyi, M. A. (2015). Continuous auditing — a new view audit analytics and continuous audit: looking toward the future. New York: AICPA 3–51.

Ciborra, C. U. (1997). De profundis? Deconstructing the concept of strategic alignment. *Scandinavian journal of information systems*, *9*(1), 2.

Coole, M., Corkill, J., & Woodward, A. (2012). Defence in Depth, Protection in Depth and Security in Depth: A Comparative Analysis Towards a Common Usage Language. (5th ed.).

Cockcroft, Steven. "What is the NIST Framework?." ITNOW 62.4 (2020): 48-49.

Creswell, J. W. (2014). Research design: Qualitative, quantitative and mixed methods approaches (4th ed.). Thousand Oaks, CA: Sage.

De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems*, *27*(1), 307-324.

Del Castillo-Peces, C., Mercado-Idoeta, C., Prado-Roman, M., & del Castillo-Feito, C. (2018). The influence of motivations and other factors on the results of implementing ISO 9001 standards. *European Research on Management and Business Economics*, *24*(1), 33-41.

Deloitte. (2017). Cybersecurity and the role of internal audit. Retrieved 2 February 2020, from https://www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-internal-audit-role.html.

Devos, J., & Van de Ginste, K. (2014). A Quest for Theoretical Foundations of COBIT 5. In *Proceedings of the European Conference on Information Management & Evaluation* (pp.73-80).Retrievedfromhttp://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=99225116&site=ehostlive.

Drljača, D., & Latinović, B. (2017). Frameworks for Audit of an Information System in Practice. *JITA - Journal of Information Technology and Applications (Banja Luka) - APEIRON*, *12*(2). doi:10.7251/jit1602078d.

Ebimobowei, A., Kereotu, O. J., & Brass Island, P. M. B. (2011). Role theory and the concept of audit expectation gap in South-South, Nigeria. *Current Research Journal of Social Sciences*, *3*(6), 445-452.

Evans, A. (2022). Cybersecurity auditing. *Enterprise Cybersecurity in Digital Business*, 252–268. https://doi.org/10.4324/9781003052616-26.

Goertzen, M. J. (2017). Introduction to quantitative research and data. *Library Technology Reports*, *53*(4), 12-18.

Goodnight, J. H. (1980). *Tests of hypotheses in fixed effects linear models. Communications in Statistics-Theory and Methods, 9(2), 167-180.*

Goldman, H. H. (2005). The origins and development of quality initiatives in American business. The TQM Magazine.

Halbouni, S. S. (2015). The Role of Auditors in Preventing, Detecting, and Reporting Fraud: The Case of the U nited A rab E mirates (UAE). *International Journal of Auditing*, *19*(2), 117-130.

Hay, D. (2014). Auditing, International Auditing and the International Journal of Auditing: Editorial. *International Journal of Auditing*, *18*(1), 1-1. doi:10.1111/ijau.12020.

Hindin, M. J. (2007). Role theory. *The Blackwell encyclopedia of sociology*.

Holden, M. T., & Lynch, P. (2004). Choosing the Appropriate Methodology: Understanding Research Philosophy. *The Marketing Review*, *4*(4), 397–409. doi: 10.1362/1469347042772428.

Ibrahim, A., Valli, C., Mcateer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: A case study. *Journal of Supercomputing, 74*(10), 5171-5186. doi:10.1007/s11227-018-2479-2.

IIA, (2012). International standards for the professional practice of internal auditing (Standards).https://na.theiia.org/standardsguidance/Public%20Documents/IPPF%202013%20English.pdf. Retrieved 04/07/2018.

IIA, (2018). Definition of internal auditing. https://na.theiia.org/standards-guidance/mandatory guidance/Pages/Definition-of-Internal-Auditing.aspx. Retrieved 30/04/2018.

IIA. (2010). *Core competencies for today's internal auditor*. Institute of internal auditors. Retrieved from https://na.theiia.org/iiarf/Public%20Documents/Core-Competencies-for-Todays-Internal-Auditor.pdf.

ISACA, & Protiviti. (2020). Today's toughest challenges in IT audit: tech partnerships, talent, transformation. Retrieved 2 March 2020, from https://www.protiviti.com/sites/default/files/united_states/insights/8th-annual-it-audit-benchmarking-survey-isaca_protiviti.pdf.

ISACA. (2015). Cyber security audit. *Isaca Journal*, *6*. Retrieved from https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpacys.

ISACA. (2019). Test your skills and take your career to the next level. *Trends, challenges and audit in a rapidly changing landscape, 6*.

Islam, M. S., Farah, N., & Stafford, T. F. (2018). Factors associated with security/cybersecurity audit by internal audit function: An international study. *Managerial Auditing Journal*.

Ittonen, K. I. M. (2010). A Theoretical Examination of the Role of Auditing and the Relevance of Audit Reports. In *Proceedings of the University of Vaasa. Teaching Aid Series* (Vol. 28,pp. 1–70). Vaasa, Finland.

Jamison, J., Morris, L., & Wilkinson, C. (2018). The future of cyber security in internal audit. Retrieved 13 May 2020, from http://theiia.mkt5790.com/FutureofCybersecurityinInternalAudit.

Jibrin, M. S., Blessing, S. E., & Danjuma, I. (2014). The role of auditors in the recent Nigerian Banking Crisis. *International Journal of Academic Research in Business and Social Sciences, 4*(3). https://doi.org/10.6007/ijarbss/v4-i3/703.

Jizi, M. I., Salama, A., Dixon, R., & Stratling, R. (2014). Corporate governance and corporate social responsibility disclosure: Evidence from the US banking sector. *Journal of business ethics*, *125*(4), 601-615.

Joshi, V., & Goyal, K. (2011). A Study of Social and Ethical Issues in banking industry. *International Journal Of Economics And Research*, *2*. Retrieved from http://www.ijeronline.com.

Jreissat, E. R., Gall, J. M., & Doheir, M. (2018). A Review of IT Audit, ITG / ISG and Cobit Frameworks on Institutions in “ MENA ” Region. *International Journal of Pure and Applied Mathematics*, *119*(18), 525–541.

Kahyaoglu, S. B., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*.

Kankam, P. K. (2019). The use of paradigms in information research. Library & Information Science Research, 41(2), 85-92.

Karam, C.M., & Ralston, D.A. (2016). "A failure before analysis: the soup to nuts of preparing for multicountry analyses", *Cross Cultural & Strategic Management*, 23(4), 590-612. https://doi.org/10.1108/CCSM-05-2016-0105.

Kolk, K. (2017). The role of auditors and information technology (dissertation). Kothari, C. R. (2004). Research methodology: Methods and techniques. New Age International.

Krumay, B., Bernroider, E. W., & Walser, R. (2018). Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST cybersecurity framework. In Nordic Conference on Secure IT Systems (pp. 369-384). Springer, Cham.

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal Of Global Information Technology Management*, *22*(2), 77-81. doi: 10.1080/1097198X.2019.1603527.

Lakens, D. (2013). Calculating and reporting effect sizes to facilitate cumulative science: A practical primer for t-tests and ANOVAs. Frontiers in Psychology, 4. doi:10.3389/fpsyg.2013.00863.

Lakens, D. (2016). Equivalence Tests: A Practical Primer for t-Tests, Correlations, and Meta-

Analyses. *Social Psychological and Personality Science*, *8*(4). doi: https://doi.org/10.1177/1948550617697177.

Lapalme, J., Kabiwa, V., & Tardif, P.-M. (2019). Relationship between information technology auditors and Auditees and their impacts on auditors. *International Journal of Engineering Business Management*, *11*, 184797901987898. https://doi.org/10.1177/1847979019878980.

Leavy, P. (2019) Research Design: Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches 1st Edition.

Levers, M.-J. D. (2013). Philosophical Paradigms, Grounded Theory, and Perspectives on Emergence. *SAGE Open*, *3*(4), 215824401351724. doi: 10.1177/2158244013517243.

Li, X. (2017). A review of motivations of illegal cyber activities. *Kriminologija & socijalna integracija: časopis za kriminologiju, penologiju i poremećaje u ponašanju*, *25*(1), 110-126.

Lloyd, I. (2020). *Information technology law*. Oxford University Press.

Mahzan, N., & Hassan, N. A. B. (2015). Internal Audit of Quality in 5s Environment: Perception on Critical Factors, Effectiveness and Impact on Organizational Performance. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, 5(1), 92-102.

Marchant, M., & Mosiana, M. (2020). The Auditors, Corporations and crime report [Internet]. Cape Town: Open Secrets; 2020 pp. 6-31. Available from: https://www.opensecrets.org.za/site/wp-content/uploads/CECR-Vol.-2_The-Auditors_Open-Secrets_July-2020.pdf.

Matsikidze, H., & Kyobe, M. (2020). A Proposed Cyber security framework for auditing in financial institutions. In *2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (pp. 0276-0281). IEEE.

McDonald, R. P. (2013). *Test Theory A Unified Treatment* (1st ed.). London: Taylor and

Francis. doi: https://doi.org/10.4324/9781410601087.

Meeker, W. Q., & Escobar, L. A. (1998). *Statistical methods for reliability data*. New York: Wiley.

Meriah, I., & Rabai, L. B. A. (2019). Comparative study of ontologies based ISO 27000 series security standards. *Procedia Computer Science*, *160*, 85-92.

Mihret, D. G., & Grant, B. (2017). The role of internal auditing in corporate governance: a guidance/Pages/Definition-of-Internal-Auditing.aspx. Retrieved 30/04/2020.

Mishra, P., Pandey, C. M., Singh, U., & Gupta, A. (2018). Scales of measurement and presentation of statistical data. Annals of cardiac anaesthesia, 21(4), 419.

Ndlovu, S. L., & Kyobe, M. E. (2016). Challenges of CoBIT 5 IT Governance Framework Migration. In *CONF-IRM.* (p. 58).

Osamah, A., Mazen, S., & Helal, I. (2018). Cyber Security Tools for IS auditing. In *the 6th international conference on enterprise systems*. Cyprus: Research gate. Retrieved from https://www.researchgate.net/publication/327369940.

Otero, A. R. (2019). *Information Technology Control and Audit*. taylor & francis group. https://doi.org/10.1201/9780429465000.

Owolabi, S. A., & Olagunju, A. O. (2020). Historical Evolution of Audit Theory and Practice. *EVOLUTION*, *16*(1).

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.

Patten, M. L., & Newhart, M. (2017). *Understanding research methods: An overview of the essentials*. Routledge.

Queirós, A., Faria, D., & Almeida, F. (2017). Strengths and limitations of qualitative and quantitative research methods. *European journal of education studies*.

Ramsarghey, K., & Hardman, S. G. (2020). The auditing profession's role in terms of accountability: a South African perspective. *Southern African Journal of Accountability* *and Auditing Research*, *22*(1), 39-49.

Razana, M., & Shafiuddin, Z. (2016). Cyber security Malaysia: Towards becoming a national certification body for information security management systems internal auditors. *International Journal Of Computer And Systems Engineering*, *10*.

Roberts, P. (2013). U.S. Cyber Security Framework Is Good News-For Hackers. Retrieved May 22, 2020, from https://securityledger.com/2013/09/u-s-cyber-security-framework-is-good-news-for-hackers/.

Sabillon, R. (2018). A Practical Model to Perform Comprehensive Cybersecurity Audits. *Enfoque UTE*, *9*(1), 127-137.

Saunders, M., Lewis, P., & Thornhill, A. (2009). Research methods for business student (4th Ed.). London: Prentice Hall.

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th ed.). Harlow: Pearson education.

Shen, L. (2014). The NIST cybersecurity framework: Overview and potential impacts. *Scitech Lawyer*, *10*(4), 16.

Shi, W., Connelly, B. L., & Hoskisson, R. E. (2017). External corporate governance and financial fraud: Cognitive evaluation theory insights on agency theory prescriptions. *Strategic Management Journal*, *38*(6), 1268-1286.

Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. *Managerial Auditing Journal*, *33*(4), 410-424. doi:10.1108/maj-07-2017-1596.

Steuperaert, D. (2019). COBIT 2019: A significant update. EDPACS, 59(1), 14-18.

Susana, T., & Pereira, M. (2018). A Security Framework for Audit and Manage Information System Security, (October 2010). https://doi.org/10.1109/WI-IAT.2010.244.

Taber, K. S. (2018). The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. Res Sci Educ 48, 1273–1296 (2018).

https://doi.org/10.1007/s11165-016-9602-2.

Taherdoost, H. (2016). Sampling methods in research methodology; how to choose a sampling technique for research. How to choose a sampling technique for research (April 10, 2016).

Tamimi, M., Aljohani, R., Alzahrani, A., & Alharbi, B. (2019). *SECURITY REVIEW BASED ON ISO 27000/ ISO 27001/ ISO 27002 STANDARDS: A CASE STUDY RESEARCH*. At Istanbul, Turkey: Proceedings of Researchfora 48th International Conference.

Tarek, M., Mohamed, E. K., Hussain, M. M., & Basuony, M. A. (2017). The implication of information technology on the audit profession in developing country: Extent of use and perceived importance. International Journal of Accounting & Information Management, 25(2), 237-255.

Tarí, J. J., Molina-Azorín, J. F., & Heras, I. (2012). Benefits of the ISO 9001 and ISO 14001 standards: A literature review. *Journal of Industrial Engineering and Management (JIEM)*, *5*(2), 297-322.

Tariq, N. (2018). Impact of cyberattacks on financial institutions. *Journal of Internet Banking and Commerce*, *23*(2), 1-11.

United Nations. Economic Commission for Africa. (2014). *Economic report on Africa 2014: Dynamic Industrial Policy in Africa*. ECA IR Home. Retrieved February 4, 2021, from https://hdl.handle.net/10855/22180.

Van de Weijer, S., Leukfeldt, R., & Van der Zee, S. (2020). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal*.

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behavior. *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2017.05.038.

Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. *The African Journal* *of Information and Communication*, *20*, 113-132.

Vaske, J. J., Beaman, J., & Sponarski, C. C. (2017). Rethinking internal consistency in Cronbach's alpha. *Leisure sciences*, *39*(2), 163-173.

Vitolla, F., Raimo, N., & Rubino, M. (2020). Board characteristics and integrated reporting quality: an agency theory perspective. *Corporate Social Responsibility and Environmental Management*, *27*(2), 1152-1163.

Ware, J. E., & Gandeka, B. (1998). Methods for Testing Data Quality, Scaling Assumptions, and Reliability: The IQOLA Project Approach. *Journal of Clinical Epidemology, 51*(11), 945–952. https://doi.org/10.1016/S0895-4356(98)00085-7.

Wertheim, S. (2019). Auditing for cybersecurity risk. *The CPA Journal*, *89*(6), 68-71.

Yeboah, T. (2013). A Proposed Information Technology Audit Framework for Microfinance Kumasi. *Journal Of Engineering, Computers & Applied Sciences, 2(8), 1-7*. Retrieved from https://www.borjournals.com.

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education*, 48(2), 311-325.

Younas, A., & Porr, C. (2022). A step-by-step approach to developing scales for survey research. Nurse Researcher, 30(2).

APPENDICES

APPENDIX A: RESEARCH INSTRUMENT (QUESTIONNAIRE)

University of Cape Town

Department of Information Systems

Leslie Commerce Building

Upper Campus

Private Bag X3 - Rondebosch - 7701

Tel: +27 (0) 21 650 2261 Fax: +27 (0) 21650 2280

Cyber security auditing Survey

IT auditing is defined as the official, liberated, and objective inspection of an organization's IT infrastructure to regulate whether the activities involved in collecting, processing, storing, transmitting and using information comply with guiding principles, safeguard assets, maintain data integrity and operate effectively and efficiently to achieve an organization's overall goals (ISACA, 2019). Cyber security audits help to identify threats and vulnerabilities, weaknesses, thereby exposing weaknesses and high-risk practices.

This is a confidential questionnaire. Therefore, the questionnaire and the information it contains will only be available to the researcher. The questionnaire also excludes the collection of personal / private information therefore, it is anonymous. Answering this questionnaire is completely voluntary and you may, at any time, decide to exit. Completing it will take approximately 12 minutes of your time. Please tick in the relevant checkbox provided.

SECTION A: General information – Demographics

1.1.Age range	18-20 years	20-30 years	30- 40 years	40-50 years	50+ years
1.2. Highest level of education	Diploma	Bachelor's degree	Master's degree	Doctoral degree	Other: Specify
1.3. Certifications	CISA	CIA	CISSP	CFA	Other: Specify

CISA- certified information systems auditor, CIA- certified internal auditor

CISSP- certified information systems security professional, CFA- certified forensic auditor

1.4. Job title	IT Auditor	Financial Auditor	Cyber Security Professional	Forensic Auditor	Other: Specify
1.5. Job Industry	Financial Sector	Health Sector	IT Sector	Law Sector	Other: Specify
1.6.Years in the profession	1-3	3-5	5-7	7-10	10+
1.7. Location	Gauteng	Western Cape	Eastern Cape	Free State	Northern Cape
SECTION B: AUDIT FRAMEWORK ADOPTION (AND EFFECTIVENESS)					
2.1. Which of these frameworks does your audit function frequently use for cybersecurity audits? (*Choose ONLY one*).					
COBIT	NIST cyber security framework	ISO 27001:2013 standards	Trust service criteria	Other ________________	
2.2. On a scale of 1 to 5, rate how effective is the cyber security framework you identified above in performing each of these activities (1= not sure; 2 = not effective; 3= somehow effective, 4 = effective; 5 = very effective)					
2.2.1. Assessing social engineering	**1**	**2**	**3**	**4**	**5**
2.2.2. Reviewing security incident response	**1**	**2**	**3**	**4**	**5**
2.2.3. Assessing data loss prevention	**1**	**2**	**3**	**4**	**5**
2.2.4. Vulnerability assessments	**1**	**2**	**3**	**4**	**5**
2.2.5. Reviewing technological innovation process	**1**	**2**	**3**	**4**	**5**
2.2.6. Reviewing systems and applications	**1**	**2**	**3**	**4**	**5**
2.2.7. Reviewing information processing facilities	**1**	**2**	**3**	**4**	**5**
2.2.8. Reviewing management of IT and enterprise architecture	**1**	**2**	**3**	**4**	**5**
2.2.9. Reviewing client, server, telecommunications, intranets and extranets	**1**	**2**	**3**	**4**	**5**
2.3. Indicate the effectiveness of the framework you frequently use for auditing cyber security in performing the following; 1= not sure; 2 = not effective; 3= somehow effective, 4 = effective; 5 = very effective)					

2.3.1. It addresses all important aspects of auditing cyber security for any organization	**1**	**2**	**3**	**4**	**5**
2.3.2. It is very easy to use in any cyber security auditing process	**1**	**2**	**3**	**4**	**5**
2.3.3. It provides tools to audit the effectiveness of security controls in place	**1**	**2**	**3**	**4**	**5**
2.3.4. The framework provides clear benefits within and over a short time	**1**	**2**	**3**	**4**	**5**
2.3.5. Current framework can be used across different financial institutions without customizing	**1**	**2**	**3**	**4**	**5**
2.3.6. The framework clearly shows how to assess cloud computing security issues	**1**	**2**	**3**	**4**	**5**
2.3.7 Current frameworks are specific to the aspects of cyber security being audited	**1**	**2**	**3**	**4**	**5**
2.3.8 The framework provides clear guidelines to follow during auditing	**1**	**2**	**3**	**4**	**5**
2.3.9 The current cyber security frameworks are vast for effective use in IT auditing in financial institutions	**1**	**2**	**3**	**4**	**5**
2.3.10 Non-IT security experts find the current cyber security frameworks difficult to use during audits	**1**	**2**	**3**	**4**	**5**
2.3.11 Current cyber security frameworks are made difficult due to critical thinking involved when conducting cyber security audits	**1**	**2**	**3**	**4**	**5**
SECTION C: AUDITORS COMPETENCIES					
What effect does the following have on the use of frameworks for cyber security auditing? 1= not sure; 2 = no effect; 3= small effect, 4 = moderate effect; 5 = major effect)					
3.1.1. An understanding of the hardware, software and business applications in an organization which need to be audited	**1**	**2**	**3**	**4**	**5**
3.1.2. Ability to analyze data to identify information to support my audit conclusions	**1**	**2**	**3**	**4**	**5**

3.1.3. An understanding of the cyber security audits and technologies involved.	**1**	**2**	**3**	**4**	**5**
3.1.4. Choosing a cyber-security framework that fits the skills of the personnel in the audit team	**1**	**2**	**3**	**4**	**5**
3.1.5. Being restricted to a single cyber security framework due to lack proper IT auditing skills	**1**	**2**	**3**	**4**	**5**
3.1.6. Avoiding using current cyber security frameworks because they are vast for effective IT auditing	**1**	**2**	**3**	**4**	**5**
3.1.7. Relying on one cyber security frameworks that the IT auditor is familiar with	**1**	**2**	**3**	**4**	**5**
3.1.8. The organizational skills of the IT auditor in using cyber security frameworks	**1**	**2**	**3**	**4**	**5**
3.1.9. The competence of IT audit team conducting internal audit	**1**	**2**	**3**	**4**	**5**
SECTION D: AUDITORS ETHICS AND INTEGRITY **4.1 How effective is your chosen framework in enhancing your integrity and ethical capabilities? Please rate each of the statement on the scale:** 1= not sure; 2 = not effective; 3= somehow effective, 4 = effective; 5 = very effective)					
4.1.1. Current cyber security frameworks require IT auditors who value ethics and confidentiality when performing audits	**1**	**2**	**3**	**4**	**5**
4.1.2. Current cyber security frameworks can assist IT auditors to maintain professional integrity during the auditing process	**1**	**2**	**3**	**4**	**5**
4.1.3. It is easy to maintain confidentiality of enterprise data and findings of an audit process when using current cyber security frameworks	**1**	**2**	**3**	**4**	**5**
4.1.4. Current cyber security frameworks cater for all ethical issues for IT auditing in financial institutions	**1**	**2**	**3**	**4**	**5**
4.1.5. Strict ethical issues demanded by existing current cyber security frameworks deter their use by IT auditors in financial institutions	**1**	**2**	**3**	**4**	**5**

SECTION E: QUALITY CYBER SECURITY AUDITS Please rate the statements below on their effectiveness in ensuring quality cyber security audits. 1= not sure; 2 = not effective; 3= somehow effective, 4 = effective; 5 = very effective)					
4.1.1. IT auditors cannot prescribe a framework to be used for their cyber security audits	1	2	3	4	5
4.1.2. l am highly confident with the effectiveness of IT audit reports on threats and vulnerabilities	1	2	3	4	5
4.1.3. Employee training to raise information security awareness is always done in my organization and l am highly satisfied	1	2	3	4	5
4.1.4. Systems and security patches are essential internal issues that the IT auditing should focus on most of the time	1	2	3	4	5
4.1.5. Social engineering audits always forms part of cyber security audits in my organization	1	2	3	4	5
4.1.6. It is a good practice that company maintain security or other certifications, (ISO 27001) for IT auditing purposes	1	2	3	4	5
Please provide any comments that can be of help to this research study. Your input is highly appreciated. ____ ____ THANK YOU					

APPENDIX B: CONSENT FORM AND COVER LETTER

Department of Information Systems
Leslie Commerce Building, Upper Campus
University of Cape Town
Private Bag X3, Rondebosch 7701
Tel. +27(0)21 - 650 2261
https://www.commerce.uct.ac.za/InformationSystems/

Request to conduct research participation consent form

Dear Sir/Madam,

In terms of the requirements for completing a Master's degree in Information Systems at the University of Cape Town, a research study is required.

The researcher, in this case (Hezel Matsikidze) has chosen to conduct a study entitled "A proposed cyber security framework for auditing in financial institutions." The objectives of this study is to improve the effectiveness of cyber security audits thereby identifying factors that enhance cyber security audits in financial institutions.

No personal identification information or of your company will be requested in the questionnaire hence anonymity is guaranteed. Your participation is entirely voluntary, and you are free to withdraw at any point should you not feel comfortable participating in the study. All the data collected will only be used for academic purposes and findings will be presented to the University of Cape Town as part of the completed dissertation. You can choose to withdraw from the research at any time for whatever reason, in accordance with ethical research requirements.

The data collection method will be a questionnaire. If you are willing to participate in this study, kindly sign the attached form and return to me. Should you have any questions regarding this research, please feel free to contact me on +27849486317 or email hezelmatsikidze@gmail.com.

Your participation in this study would be greatly appreciated.

Sincerely,

Hezel Matsikidze
Masters Student
Department of Information Systems
University of Cape Town
Contact: hezelmatsikidze@gmail.com

Prof Michael Kyobe
Research Supervisor
Department of Information Systems
University of Cape Town
Contact: Michael.kyobe@uct.ac.za

APPENDIX C: ETHICS CLEARANCE FORM

Faculty of Commerce

Private Bag X3, Rondebosch, 7701
2.26 Leslie Commerce Building, Upper Campus
Tel: +27 (0) 21 650 4375/ 5748 Fax: +27 (0) 21 650 4369
E-mail: jacques.rousseau@uct.ac.za
Internet: www.uct.ac.za
@Commerce UCT **UCT Commerce Faculty Office**

02/10/2020

Hezel Matsikidze

Department of Information Systems

University of Cape Town

REF: REC 2020/10/002

A proposed cyber security framework for auditing in financial institutions.

We are pleased to inform you that your ethics application has been approved. Unless otherwise specified this ethical clearance is valid until 31-Oct-2021 .

Your clearance may be renewed upon application.

Please be aware that you need to notify the Ethics Committee immediately should any aspect of your study regarding the engagement with participants as approved in this application, change. This may include aspects such as changes to the research design, questionnaires, or choice of participants.

The ongoing ethical conduct throughout the duration of the study remains the responsibility of the principal investigator.

We wish you well for your research.

2020.10.02
14:46:36 +02'00'

Jacques Rousseau
Commerce Research Ethics Chair
University of Cape Town
Commerce Faculty Office
Room 2.26 | Leslie Commerce Building

Office Telephone: +27 (0)21 650 2695 / 4375
Office Fax: +27 (0)21 650 4369
E-mail: jacques.rousseau@uct.ac.za
Website: https://www.commerce.uct.ac.za/Pages/Ethics-in-Research

"Our Mission is to be an outstanding teaching and research university, educating for life and addressing the challenges facing our society."

APPENDIX D: DATA COLLECTION APPLICATION- ISACA

ISACA South Africa Chapter

Roodebloem Office Park
20 Bella Rosa Street
Bellville
Cape Town
7535

19 Maxwell Office Park
Mac Mac Building
Waterfall City
Midrand
Johannesburg
2090

ISACA SA Research Assistance Programme

Purpose:

The purpose of the programme is to provide students who are in their final year or pursuing post graduate studies in areas where there is potential to advance the Chapter's programmes with access to a database of potential research participants, thus not only helping the students to advance their studies, but also contributing to the creation of knowledge. Applicants for Research Assistance must note that members of ISACA SA to whom we will direct the survey tools are encouraged to, but do not have an obligation to participate in the research assistance program.

Students interested in applying for Research Assistance support must complete this application form and submit supporting information requirements as noted below to ***academic.relations@isaca.org.za*** *and* ***info@isaca.org.za***

Rules

1. Ethical Clearance form from the University at which the student is enrolled (survey will not be sent to our members without the ethical clearance).
2. Preference will be given to students pursuing the fields of Information Systems (IS), Cybersecurity, IT Governance, IT Audit, IT Risk Management, Information Security, Information Technology, Internal Audit, Accounting, Financial Information Systems or other related studies.
3. All Applicants must be registered for the relevant academic year in respect of University students (proof of registration required)
4. Students who submit a recommendation letter from their University, a member of ISACA, their mentor, or another professional body will be given preference

NB: ISACA SA may at its discretion offer a letter of support to facilitate issuance of an ethical clearance by the University where required, but the survey tool will only be sent to the research participants in our database once such ethical clearance has been received by ISACA SA. Such letter of support will only be granted after this application form has been duly completed.

ISACA
South Africa Chapter

Boodakloem Office Park
20 Bella Rosa Street
Bellville
Cape Town
7535

19 Maxwell Office Park
Mac Mac Building
Waterfall City
Midrand
Johannesburg
2090

Section 1 – Administrative Information

Name(s) & Surname:	Hezel Matsikidze
University Name	University of Cape Town
Field of Study & Expected Date of completion	Masters in information systems 30/11/2021
Home or Campus Address: (optional)	2 Sydney road, Mowbray, Cape Town, 7700
Postal Address:	30 FRANK ROBB, BROOKLYN, CAPE TOWN, 7405
Home or Campus Phone:	+27 (0)216504375
Cell Phone Number:	+27849486317
Email Address:	hezkay123@gmail.com mtshez001@myuct.ac.za

ISACA South Africa Chapter

Boodebloem Office Park
20 Bella Rosa Street
Bellville
Cape Town
7535

19 Maxwell Office Park
Mac Mac Building
Waterfall City
Midrand
Johannesburg
2090

Section 2 – Activities and Interests

A. List and briefly describe *volunteer* activities in which you have been involved:

Organisation Name	Position Held (Dates)	Description
Bethesda Apostolic church	Sunday School teacher	Engage, teach and spend time with children
Redcliff community	Academic teacher	I offered free lessons to school children from my community

B. List honours or *academic awards* you have received (e.g. scholarly activities, research, etc.):

Award/Honor	Institution/Organisation	Date(s)
Merit award	University of Fort Hare	03/03/2018
Best academic tutor	University of Fort Hare	03/03/2018
Published research paper	IEEE Explore	02/12/2020

C. List and briefly describe your *extracurricular* activities if any (e.g. memberships in Organisations, sports, etc.):

Organisation Name	Dates	Description (including positions held as applicable)
Milnerton tennis sports club member		Member of the tennis sports club
IITPSA	15/032/2018	Student member of the institution

ISACA
South Africa Chapter

Boodabloem Office Park
20 Bella Rosa Street
Bellville
Cape Town
7535

19 Maxwell Office Park
Mac Mac Building
Waterfall City
Midrand
Johannesburg
2090

Section 4 – Consent to publish results of Research

B. Indicate by answering **yes** or **no** in the box below whether you give ISACA SA at its discretion, permission to publish the results of your research through its website, social media pages or any other platform

NB: This information will not be used against applicants but ISACA would be better able to fulfil the objective of facilitating knowledge creation if we can optionally publish some of the research results where necessary.

ISACA SA Will also notify the relevant authors of such intention to publish before doing so at the relevant time.

No

Section 5 – Communication of outcome of application

Applications for Research Assistance shall be approved by the Academic Relations and Education Committee and its decision regarding whether or not to support the application shall be considered final. Applicants should allow a turnaround of a maximum of two weeks to receive feedback on their applications (i.e. within 1-14 days).

____Hezel Matsikidze________________________ 03/03/2021__

Signature of Applicant **Date**

APPENDIX E: ISACA DATA COLLECTION APPROVAL LETTER AND EMAIL

ISACA
South Africa Chapter

Roodebloem Office Park
20 Bella Rosa Street
Bellville
Cape Town
7535

Re: ISACA SA letter of confirmation of Research Assistance Support

We confirm that Hazel Matsikidze, a Masters in information systems student at the University of Cape Town, submitted an application for research assistance support on the 3rd of March 2021. Specifically, she requested permission to use the ISACA SA Chapter's membership database as a platform to distribute her data collection instrument / questionnaire for her research. ISACA SA responded to her through email on the 17th of March 2021, approving the request.

This letter serves to formally confirm the approval we gave her through email on the 17th of March 2021.

The approval is in keeping with one of ISACA SA's objectives to facilitate the creation of industry enriching knowledge by providing research assistance to students in their final year studies or pursuing post graduate studies in areas where there is potential to advance the Chapter's programmes.

Yours Faithfully,

Edmore Taruvinga
Academic Relations & Education Director (ISACA SA)

Edmore Taruvinga | ISACA SA Chapter Academic Relations & Education Director <academic.rel... Mar 17, 2021, 7:19 AM

to Arlene-Lynn, Eugene, me

Good Morning Hazel,

We have gone through you application pack and i am pleased to inform you that ISACA SA will be able to provide the requested support in terms of distributing your research instrument / questionnaire to our member database.

Kindly note that while we encourage our member database to provide assistance in terms of responding to research questionnaires, the actual decision either to respond or not is entirely up to them.

We will hear from you once you are ready to disseminate your questionnaire.

Thank you,

Regards