The application of digital ethics practices to mitigate digital fraud in a Mobile Network Operator in South Africa

Simile Ndlovu

A research report submitted to the Faculty of Commerce, Law and Management, University of the Witwatersrand, in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business

Johannesburg, 2024

ABSTRACT

The internet has allowed for the existence of digital advancements like social media, online shopping, online banking, and online learning, among other conveniences. Equally, the internet has brought about phishing, malware, identity fraud, application fraud, and other cybercrimes. Due to the affordance created by the internet, society cannot simply walk away from it. The focus of the study was that the lack of adoption of digital ethics practices leads to possible digital fraud because the risks of digital technologies are not mitigated. The theory adopted was the stakeholder theory, which places an ethical duty on the organisation not to harm stakeholders. The organisation's failure to maintain a balance between the positive and negative of digital technologies might cause harm of digital fraud. Thus, the adoption of digital ethics practices ensures success in the market and the introduction of control measures to mitigate digital fraud.

The study adopted a qualitative research approach, data was collected through semi-structured interviews with 12 management level employees of Company X, who are involved in the management and implementation of digital technologies, products or solutions, digital fraud, and digital ethics.

Several challenges were highlighted in the study relative to the research questions. The study found that Company X's digital ethics framework and governance were not implemented. Some of the Company X digital ethics practices are aligned with the requirements of the literature, and some require varying improvements. However, the absence of a framework and governance was negating some of the digital ethics practices. Thus, the practices are not intentional, matured, structured, or uniformed.

The study concluded that the non-implementation of the digital ethics framework and the lack of governance of digital ethics might amplify the creation of digital fraud to customers and members of the public. Since digital ethics practices are not guided, this may compromise the delivery of the digital initiatives including the digital strategy. To address the said challenges, four recommendations were made, namely, the enhancement of the organisational culture, the implementation of the digital ethics framework, the implementation of the governance of digital ethics, and the enhancement of the risk and fraud risk management processes.

KEYWORDS

Digital ethics, digital fraud, Mobile Network Operators, risk management.

DECLARATION

I, **Simile Ndlovu,** declare that this research report is my own work except as indicated in the references and acknowledgements. It is submitted in partial fulfilment of the requirements for the degree of Master of Management in the field of Digital Business at the University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

Name: Simile Ndlovu

Signature: 

Signed at Johannesburg, on the 14 day of February 2024

DEDICATION

To my late grandmother, Khefi Dlamaga Mahlangu, ngiyathokoza Mgwezane for your selfless love and sacrifices. To my late parents, Norman and Senzi Ndlovu, thank you for the discipline and the solid upbringing that you gave me.

ACKNOWLEDGEMENTS

The completion of my studies would have not been possible without the support and understanding of these people. They contributed and gave me the strength to complete my studies. I therefore wish to thank the following:

- My supervisor, Professor René Pellissier, for supporting and guiding me to complete my studies on time.

- My immediate and extended family, for being supportive and understanding while I was writing the research project.

- My friend Michael Mthombeni, for always encouraging and motivating me to push harder and harder on everything that I do.

- My friend Dr Humphrey Sithebe, for setting the bar very high and the intellectual discussions that kept me motivated throughout.

- My manager, Malebu Makgalemela Mogohloane, for the support, understanding and contribution that she made during my studies.

- My former manager, Dr Pat Mazibuko, for the encouragement, words of wisdom and for pushing me to study for this qualification and beyond.

- Lastly, all my colleagues and fellow students at WBS who provided valuable insights, information and support, and utmost gratitude to all colleagues who participated in the study.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

ACRONYM	DESCRIPTION
AD	Active Directory
AI	Artificial Intelligence
ACT	Association of Communication Technology
BASA	Banking Association of South Africa
BU	Business Unit
CAPEX	capital expenditure
CEO	Chief Executive Officer
COMRiC	Communication Risk Information Centre
COVID-19	Corona Virus Disease 2019
CRC	Commercial Review Committee
DEF	Digital Ethics Framework
DEGC	Digital Ethics Governance Committee

DEO	Digital Ethics Officer
FRM	Fraud Risk Management
GRC	Governance Risk Committee
ICASA	Independent Communication Authority of South Africa
ID	Identity Document
IEEE	The Institute of Electrical and Electronics Engineers
IoDSA	Institute of Directors South Africa
IoT	Internet of Things
IS	Information Security
ISC	Information Technology Steering Committee
IT	Information Technology
ITEB	Information Technology Executive Board
LLM	Large Language Models
ML	Machine Learning
MNO	Mobile Network Operator

NCA	National Credit Act
NGO	Non-Governmental Organisation
NPO	Non-Profit Organisations
OTP	One-Time Password
POPIA	Protection of Personal Information Act
PRECCA	Prevention and Combatting of Corrupt Activities
PSC	Project Steering Committee
RC	Risk Committee
RPA	Robotic Process Automation
SABRIC	South African Banking Risk Information Centre
SAFPS	South African Fraud Prevention Services
SAPS	South African Police Services
SEC	Social and Ethics Committee
UK	United Kingdom

URS	User Requirements Specification
USA	United States of America
VPN	Virtual Private Network
WEF	World Economic Forum
WfH	Working from Home

CHAPTER 1. INTRODUCTION

This chapter outlines the statement of purpose, background, research problem, research questions, rationale, delimitations of the study, definition of terms, and assumptions.

1.1 Statement of purpose

This study explores the application of digital ethics practices to mitigate digital fraud in a Mobile Network Operator (MNO) in South Africa. This is a qualitative research methodology study in a selected Mobile Network Operator (MNO) in South Africa, referred to in this report as Company X.

1.2 Background of the study

Responsible corporate citizenship requires that organisations as creators and adopters of the new digital technologies ensure that their application and use do not harm their stakeholders. According to Wellard (2022), this makes digital ethics as important as digital transformation itself. Market demands and pressures force for-profit organisations to be in constant search of better ways to outsmart the competition. To that end, organisations are looking to opportunities presented by Fourth Industrial Revolution digital technologies to optimise operations and to better serve customers and the broader society. The advent of the Corona Virus Disease 2019 (COVID-19) accelerated digital transformation; as a response to this exogenous change, organisations are adopting digital technologies and service offerings to remain relevant in the market (Deloitte, 2020).

As organisations embark on digital transformation, they must embed digital ethics principles, to ensure that there is an analysis of the positives and the negatives introduced by digital solutions (Becker et al., 2022). This will ensure that organisations equally address both the digital transformation and the digital ethics imperatives. This view is also supported by PWC (2022), who indicated that as organisations pursue digital transformation, they need to address both sides, that is, weighing enhancing

customer experience and the prevention of fraud. Detura et al. (2022) posit that organisations make a trade-off between superior digital services offerings and digital fraud prevention. This means that organisations struggle to enhance fraud controls without impacting customer experience and vice-versa.

The 2024 World Economic Forum (WEF) global risks report highlighted the downsides posed by digital technologies or Artificial Intelligence (AI) risks. According to Torkington (2024), some of the negatives of digital technologies are misinformation, cybercrime, cyberattacks, and job losses. These risks are further exacerbated by the fact that there has been a concerted focus on innovation, but without a corresponding focus on the regulation of digital technologies (Torkington, 2024). The concerns of AI are driven by the emergence of ChatGPT, and other large language models (LLM) have raised the need for digital ethics for the benefit and protection of society (Li, 2023)

The MNO industry is a capital expenditure (CAPEX) heavy industry because of the investment required for the network infrastructure. The industry had to fast-track digital transformation as a means of reducing the cost of doing business. Despite the increasing demand for MNO services, their revenue margins have been declining (Deloitte 2020; Schiff et al., 2020). Amidst the increasing number of smartphone users and demand for data services, the MNOs are facing challenging market conditions mainly because of weaker economy, compounded by load-shedding, unemployment, and global geo-political issues that have affected the availability and supply of devices (Deloitte, 2020). To deal with these challenges, MNOs are using AI and Machine Learning (ML) to improve customer experience (PWC, 2023). More recently, generative AI like LLM has been used to perform some of the corporate functions.

According to PWC (2022), the wide adoption of digital technologies has corresponded with an increase in digital fraud cases. Digital fraud is a subset of cybercrime, and it is pervasive in nature. It is found in banking, insurance, retail, MNOs, and many other sectors of the economy. The PWC 2022 global fraud report and the South African Fraud Prevention Services (SAFPS) report noted that there has been an increase in cybercrime in South Africa. The PWC (2022) report found that 43% of digital fraud is perpetrated by external fraudsters, 31% by internal fraudsters, and 26% by collusion between external and internal fraudsters. The SAFPS (2023) indicated that identity

fraud has increased by 300% between 2021 and 2022. The same report noted that other types of digital fraud have also increased.

Digital fraud in the MNO industry is perpetrated mainly in two ways. Firstly, by targeting customers or members of the public, and secondly, by targeting the MNO itself (Mabuza, 2021). The customers and members of the public are targeted through various types of scams and social engineering means (Thompson, 2022). In terms of scams, in some instances, fraudsters purport to be employees or act on behalf of the MNOs. Some of those include competition scams, discounted airtime or data scams, sim-swap fraud, porting fraud, and so forth (Libera, 2022).

In the case of social engineering, the aim is to get the customer or member of the public to reveal their personal information, which is then used to commit identity or fraud (Mabuza, 2021; Thompson 2022; Babaei et al., 2020). The MNO is targeted by using the information fraudulently sourced by the fraudsters. They are targeted through various types of identity or subscription fraud activities, which are digitally perpetrated (Thompson 2022; Libera, 2020). According to Babaei et al. (2020), some of these include post-paid contract application fraud, where fraudsters use details of the victim to apply for credit with the aim of not paying for the consumed services. These types of fraud cause reputational damage to MNOs (Babaei et al., 2020)

In some instances, MNO processes are abused to enable banking fraud. Fraudulent sim-swap and porting transactions are performed on customer accounts with the aim of committing banking fraud (Libera, 2022). Once the fraudulent sim-swap or porting transaction is performed, the fraudsters would intercept the One-time Password (OTP) from the bank, to access the customer's bank account and perform fraudulent transactions (Mabuza, 2021). Some of the MNO frauds are caused by collusion between external actors and employees or third-party employees (Mabuza, 2021). This includes exploiting weaknesses in the network and application systems. Some of the fraud is made possible by sharing of logging credentials, most predominantly within the MNO customer-facing stores and call centres.

1.3 Research problem

The research problem that informs this study is as follows:

> The lack of adoption of digital ethics practices leads to possible digital fraud because the risks of digital technologies are not mitigated.

This research seeks to explore the application of digital ethics practices to mitigate digital fraud in Company X. Post Covid-19, the incumbent organisation increased its digital transformation efforts. As was noted by PWC (2022) and SAFPS (2023), Company X is also experiencing increased digital related fraud compared to pre Covid-19 period. The scourge of economic crimes like subscription fraud, theft, sabotage, and damage to critical network infrastructure like copper and fibre cables, batteries, and towers has resulted in the MNO establishing two Non-Profit Organisations (NPO); the Association of Communication Technology (ACT), and the Communication Risk Information Centre (COMRiC).

In comparison to the banking sector, ACT is the equivalent of the Banking Association of South Africa (BASA) and COMRiC is the equivalent of the South African Banking Risk Information Centre (SABRIC). The ACT board is made up of the Chief Executive Officer (CEO) of MNOs, and it deals with policy, legislative, and regulatory operating environment, including theft, damage, and sabotage of critical MNO infrastructure. COMRIC deals with economic crimes, including digital fraud. COMRiC also coordinates risk management efforts of the industry to deal with load shedding, riots, and other threats.

As indicated by PWC (2022), good digital ethics practices present an opportunity for the incumbent organisation to consider the upside (opportunities) and downside (risks) when designing and implementing a digital solution. This is illustrated through the following examples:

1. Due to a sheer number of transactions below R50. The organisation might design or configure a customer management system to automatically approve all transactions below R50. These transactions would not require the approval of a manager. The justification from the organisation might be that managers would not have time to look at all the transactions and they should rather use

the time to perform critical tasks. In the absence of segregation of duties, the digital ethics question is, how would the organisation ensure that customers are not harmed by ensuring that the transactions below R50 are free from manipulation and fraud.

2. In a drive to increase the revenue streams, an organisation might decide to offer fintech services. To increase the uptake of their fintech solution, they might decide to design an end-to-end onboarding process that is paperless. The customers can create accounts without submitting the actual copy of their identity documents (ID). This would be a convenience for the customers, from a business point of view. The digital ethics question is, what process would be in place to ensure that fraudsters do not harm ordinary members of the public, by fraudulently opening accounts on the fintech platform using their ID numbers.

The management of digital ethics must be deliberate to ensure that the creation of a digital solution to solve one problem, (quick and efficient customer onboarding), does not create a new problem (post-paid contract credit application fraud). This can be achieved through a risk-based framework that regulates the application and use of digital technologies (Anneroth, 2022). The framework must contain risk management processes to identify, measure, and monitor the downside of digitisation, including those that might unwittingly enable fraud and weaken the control environment.

1.4 Research questions

1) How is governance of digital ethics practiced in Company X?
2) What are the components of the digital ethics framework in Company X?
3) How are the risks and causes of digital fraud mitigated in Company X?

1.5 Rationale

According to Ashok et al. (2022), there is substantial evidence of abuse of digital technologies, but worryingly the research on digital ethics has been lacking. The said authors reviewed 59 research articles and found that none of those related to the impact of digital ethics on digital fraud specifically. The literature review conducted did not find research that was specifically related to the topic of this research.

This study concluded interviews with Company X management-level employees involved with the application of digital technologies, digital fraud, and digital ethics. The outcome of this study can be adopted by Company X to enhance digital ethics governance, framework, and general digital ethics practices. The contribution of this study is that it will add to the discussion about digital ethics; it will provide a deeper, but narrow perspective about digital ethics practices to mitigate digital fraud in an MNO.

1.6 Delimitations of the study

a) This was a qualitative study focusing on Company X, one of the MNOs in SA. The study did not cover all MNOs. The research confined itself to the mobile network section of Company X, and not any Business Units or subsidiaries of Company X.
b) This research looked at practices of digital ethics to mitigate digital fraud from the business management point of view and not Information Technology (IT). The focus was on understanding the possible negative impact of digital technologies or solutions on digital fraud in Company X. The research did not focus on any downside or risk other than that of digital fraud.
c) The research focussed on the high-level processes available to manage digital ethics, covering governance; isolation of responsibility, the teams or functions involved; and the identification, evaluation, monitoring, and reporting of the downside management of digital solutions that are deployed.

1.7 Definition of terms

Table 1. Definitions of terms

Terms	Description
Digital ethics	Digital ethics is defined as: “The ethics of the application of digital technology, which takes into account the intended and unintended use and consequences of that technology, now and in the future”. (Armstrong & Lee, 2022, p. 330)
Digital fraud	Digital fraud is also known as cyber fraud, online fraud, or internet fraud. Digital or cyber fraud is the intentional misrepresentation through a computer program; or interference with data or a computer program, as or interference with a computer data storage medium or a computer system, and those actions must cause actual or potential prejudice to another person (Cybercrimes Act, 2020).
MNO	An MNO is in a sub-component of the telecommunication industry, they primarily offer wireless mobile voice and data communication services to their customers (Rouse, 2011)

1.8 Assumptions

a) It is assumed that the downside or the unintended consequence of a digital solution or transformation if not mitigated can cause harm (Becker et al., 2022). In this specific study, that harm was confined to digital fraud.
b) It is assumed that the participants accurately reflected their perspectives and experiences as subject matter experts and role players involved in issues relating to digital ethics and/or digital fraud within Company X.

1.9 Chapter Outline

This study consists of six chapters as indicated below:

Chapter One: Introduction

This chapter deals with the statement of purpose, background to the study, research problem statement, research questions, rationale, delimitations, and assumptions.

Chapter Two: Literature Review

In this chapter, the literature relevant to this study is discussed. The main sections are digital ethics, digital fraud, and the latest developments in the MNO industry. The literature and theoretical framework relating to these sections are discussed.

Chapter Three: Research Methodology

In this chapter, the research methodology is discussed. This chapter deals with the introduction, research methodology, sampling strategy, pilot testing, data collection, data processing, quality assurance, ethical considerations, and proposed timelines.

Chapter Four: Findings

In this chapter, the analysis of the research data is discussed. The findings are presented and discussed under thematic sections aligned with the research questions.

Chapter Five: Discussions

In this chapter, the findings of the research are discussed.

Chapter Six: Conclusions

In this chapter, conclusions are made based on the discussion. The conclusions are made with reference to the research questions based on the literature review and the findings.

CHAPTER 2. LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.1 Introduction

This chapter discusses and analyses the literature review of the practice of digital ethics to mitigate digital fraud. This follows the context provided in Chapter 1. The review contains empirical research, legislative framework, theoretical framework, and conceptual framework on areas relating to the study. The various concepts of this study are defined and explained. Finally, the analysis of the findings is presented, including the conclusion. According to Snyder (2019), the literature review synthesises the current body of knowledge, provides a view of frameworks and concepts that are relevant, and which will anchor the findings of the study.

2.2 Background discussion on key concepts

There are two key concepts in this study. These are digital ethics and digital fraud. These concepts are defined below.

2.2.1 Digital ethics

Armstrong and Lee (2022) indicated that digital ethics is the management of the intended and unintended consequences of the new digital technologies, now and in the future. Floridi (2018) and Ashok et al. (2022) posited that digital ethics contains hard and soft ethics, the former being compliance with regulations, and the latter being what must be done and not be done in addition to the regulatory obligations. Digital ethics was borne out of the consequences of digital technologies, which can be avoided if there is a sound application of digital ethics practices that proactively anticipates and mitigates the risks of digital technologies (Floridi, 2018).

Müller (2021) submits that the imperatives for digital ethics practices have increased in the last few years. This has led to the creation of new digital ethics jobs and

increased interest from the academic community and society in general (Müller, 2021; Eitel-Porter, 2021). This is supported by Winfield et al. (2019) and Schiff et al. (2020), who found that since 2016 there has been a growth in research output and documents on digital ethics from several role players. The growth was fuelled by concerns about the abuse of AI and its impact on humans and society (Hanna & Kazim, 2021).

Digital ethics is concerned with the development and use of digital technologies, like Blockchain, AI, Automation or Robotic Process Automation (RPA), Internet of Things (IoT), and Big Data. According to Floridi (2018) and Müller (2021), digital ethics has evolved from being called computer ethics and information ethics. AI ethics is the sub-set of digital ethics (Hanna & Kazim, 2021), this also includes data ethics and robot ethics (Müller, 2021). Digital ethics in certain quarters is being referred to as AI ethics, and the terms are used interchangeably.

Due to concerns about the abuse of digital technologies, several organisations including Google, Apple, and Amnesty International introduced AI ethics guidelines or recommendations (Jobin et al., 2019). Other guidelines were developed by the Partnership in AI, which consists of among others Google, Apple, Amazon, Facebook, IBM, and Microsoft (Winfield et al., 2019). The debate on digital ethics is intensifying; this will help forge collaborations, partnerships, and the formation of new organisations (Schiff et al., 2020). The concerns that have increased the need for the existence of digital ethics include fake news, the use of Twitter or X bots to influence Brexit and the 2016 United States of America (USA) elections, bias algorithms causing numerous forms of discrimination, the prevalence of cybercrime, malware, cryptocurrency fraud, and others (Ashok et al., 2022). These concerns can be diminished if digital ethics is not an afterthought, but a vital cog in the organisational strategy for the use of digital technologies (Floridi, 2018).

The concerns of abuse of digital technologies have caught the attention of Non-Governmental Organisations (NGOs) and countries like Denmark, the United Kingdom (UK), Canada, France, the USA and China (Schiff et al., 2020). The Chinese government has communicated its ambitions of becoming a world leader in digital technologies, specifically AI (Floridi & Cowls, 2019). There is little or no information on the position of South African and African governments on the regulation of digital ethics. The Institute of Electrical and Electronics Engineers (IEEE), which has 420,000

members in more than 160 countries, has released the ethical design standard to ensure that those who are involved in the development of digital technologies are aware of the ethical considerations of digital technologies (IEEE, 2017). Their position is that digital technologies must be developed for the betterment of humanity, they must serve humanity, and not the other way round (IEEE, 2017).

2.2.2 Digital Fraud

Crime and general unethical conduct have perennial existence in society. Fraud is a common law criminal offence. It is defined as the “unlawful and intentional making of a misrepresentation which causes actual prejudice, or which is potentially prejudicial to another” (Snyman, 2014, p523). The common law offense has four elements, which are unlawful, intention, misrepresentation, and prejudice.

Digital fraud is also known as cyber fraud, online fraud, or internet fraud, and it is a subset of cybercrime. In South Africa, digital or cyber fraud has also been made a statutory offence ("Cybercrimes Act, 19," 2020). The Cybercrimes Act (2020) definition of cyber fraud is almost the same as that of Snyman. These said elements of fraud have been carried over to the new definition of digital fraud. The difference is that the misrepresentation must be made through a computer program, or interference with data or a computer program; or interference with a computer data storage medium or a computer system; and all these must cause actual or potential prejudice or harm to another person.

Digital fraud is perpetuated using emails, websites, social media, software applications, and other digital means. It includes identity fraud and other forms of deception targeted at organisations, customers, and members of the public. The Cybercrimes Act (2020) was promulgated to deal with the scourge of digital or cybercrimes. This was imperative because fraud is the most prevalent crime in the digital era (Kemp, 2020).

Section 54 of the Cybercrimes Act (2020) has a reporting obligation for electronic communications service providers (including MNOs) and financial institutions. In terms

of that obligation, certain offences must be reported to the South African Police Services (SAPS) within 72 hours of being aware of the offence. The reportable offences fall under Part I of Chapter 2 of the Act. Some of those offences are unlawful access; unlawful interception of data; unlawful acts in respect of software or hardware tools; unlawful interference of data or computer programs; cyber fraud; cyber extortion; unlawful acquisitions, possession, provision, receipt, or use of passwords, access code or similar data or device; and unlawful interference with computer data storage medium or computer system and others.

The Cybercrimes Act (2020) augments the Prevention and Combatting of Corrupt Activities (PRECCA), Act 12 of 2004. Section 34 of PRECCA imposes reporting obligations to the police; on persons with positions of authority within organisations to report offences of fraud and other acts of criminality of R100 000 and above and of any value as far as it relates to corruption. There has been a considerable time since the PRECCA Amendment Bill of 2017 was drafted, should it become law, it will obligate organisations to conjure effective controls to ensure that fraud, theft, corruption, and other acts of criminality are prevented and detected. This is another reason why digital ethics is imperative, as it will compel organisations to put effective controls to proactively mitigate fraud-vulnerable areas caused by digital technologies.

2.3 The MNO industry in South Africa

MNOs are a sub-component of the telecommunication industry, and they primarily provide wireless mobile voice and data communication services (Rouse, 2011). The main players in the MNO industry in South Africa are Vodacom, MTN, Telkom, Cell C, and lately Rain. The MNOs are regulated by the Independent Communication Authority of South Africa (ICASA). The telecommunication industry collective revenue for 2021 was R200 billion, a decline of 0.5% from 2020, and employment decreased by 35.8% (ICASA, 2022). Despite the decline in revenue, the demand for prepaid and post-paid services has increased in 2021, compared to 2020 (ICASA, 2022).

Digital technologies anchor digital services like social media, online banking, e-learning, and e-commerce platform services. All these are enabled by the infrastructure of MNOs and other role players within the broader Information and Communication Technology (ICT) industry. Shava (2021) found that MNOs in SA have a low customer

satisfaction level and that they need to improve on that aspect to enhance their market competitiveness. The low customer satisfaction levels are compounded by high data costs, Chinembiri (2020) established that digital literacy and high data costs are the key digital divide barriers that prevent poor people from connecting to the internet. All these are happening despite some of the MNOs reducing their data costs because of the intervention by the Competition Commission and society-driven campaigns like #DataMustFall, which was waged on several social media platforms in South Africa.

Post COVID-19 MNOs have been experiencing declining margins (Deloitte, 2020). To counter that effect, they have rightfully embraced digital transformation to reduce the cost of doing business and to improve customer experience (PWC, 2023). To compensate for the declining margins, some of the MNOs are offering digital wallet payments and other fintech related services. Some MNOs are venturing into healthcare, education, insurance, and other industries. Becker et al. (2022) argued that when MNOs must not stop or slow down the good practices of digital ethics, and only focus on the positives of that digital transformation; because doing so, will expose them to digital fraud and other myriad of risks.

2.4 Digital Ethics Governance

The views of Armstrong and Lee (2022) are that technology is not passive, it has agency. After comparing the positions of ethics scholars like Floridi, Johnson, and Verbeek; Fritz et al. (2020), concurred with Johnson that digital technologies, specifically AI, do not have moral agency, because it does not have intention. This is a contrasting view compared to Floridi, who indicated that technology has moral agency, while Verbeek is of the view that humans and technology have joined moral agency, because of technical-human interactions (Fritz et al., 2020). Martinho et al. (2021) posit that one of the reasons that autonomous digital technologies cannot have moral agency is that they do not have freedom and cannot be held responsible.

Hallamaa and Kalliokoski (2020) submit that the intelligence of a technology extends to the capabilities accorded to them by human beings; that they are the product of their designs, and that they do not have the ability to discern between good and bad. Even

if technology has intention, it cannot be held accountable for its action or inaction, especially if it is autonomous and self-learning; ultimately it is the human beings that must be held accountable for its action or inaction (Hallamaa & Kalliokoski, 2020). This is consistent with the position advanced by IEEE (2017) that digital technologies are created to serve human beings, and therefore, human beings cannot abdicate their agency to them.

Martinho et al. (2021) conducted a study that measured the views of 50 ethics scholars on the moral agency of artificial and autonomous digital technologies and found that they have different views on the issue. In the main, those views can be categorised into three; those that say technologies have moral agency; those that are in the middle; and those that say it does not have moral agency (Martinho et al., 2021). The dominant view is that no matter how smart or advanced the technology can be, however, it will never be a moral agent. As postulated by Hallamaa and Kalliokoski (2020), responsibility for effective ethical design and ethical utilisation of digital technologies must be isolated to human beings. Based on that, the use of digital technologies must be governed to ensure they function in the manner they were intended.

2.4.1 *Definition*

Digital ethics governance relates to the coordination and development of policies, procedures, standards, and processes to ensure that there is sound design and transparency in the design of digital technologies and solutions (Winfield et al., 2019; Floridi, 2018). The Report on Corporate Governance 2016 (King IV) by the Institute of Directors South Africa (IoDSA), indicates that organisational governance must enable a positive ethical culture. As much as it does not mention digital ethics, King indicates the following:

> “In the context of organisations, ethics refers to the ethical values applied to decision making, conduct and the relationship between the organisation, its stakeholders and broader society” (IoDSA, 2016, p 12).

According to King IV, organisations have an obligation to effect ethical decision making in the execution of their mandate. Floridi (2018) makes a distinction between digital governance, digital ethics, and digital regulation, and posits that digital ethics is shaped

by digital governance and digital regulations**.** As indicated in Figure 1, Floridi (2018) mentioned that digital governance is shaped by digital regulation, because it is the former's responsibility to ensure that the law is complied with. Digital regulation is about what is legal or not, which is not enough, but not what is good or bad to have an impact on society. Digital ethics shapes digital governance and digital regulation, as far as it relates to them considering moral evaluation.

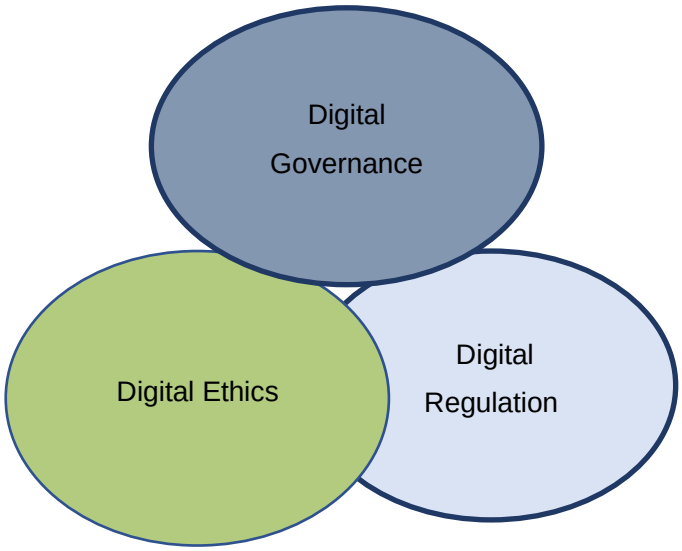

Figure 1: The relationship between digital governance, digital ethics, and digital regulation

Source: *Floridi (2018)*

As there is the absence of widespread global regulation, Li (2023) argues that like the regulation of data privacy, governments will ultimately set laws that will govern digital ethics. The said laws will have monitoring capability to ensure that organisations are complying. Stahl (2022) suggested that those laws must cater to a dedicated regulatory agency, which is similar to existing data privacy regulators.

2.4.2 *The ethical culture enables digital ethics governance*

The organisational culture describes how the organisation does things (Bamidele, 2022), and the culture can be created intentionally or unintentionally (Lubis & Hanum, 2020). The ethical culture of the organisation is the sub-set of the organisational culture; numerous ethical culture models highlighted the correct tone at the top as a common imperative for a positive ethical culture (Ndlovu, 2020). The digital ethical culture is part of the ethical culture of an organisation.

The governance of ethics is dependent on the positive ethical culture of the organisation, it would not exist in the absence of a conducive environment. Armstrong and Lee (2022) indicated that organisational culture is a foundational pillar, and to succeed in the current digital epoch, leaders must be cognisant of its significance in the organisation. This is supported by Lubis and Hanum (2020), who explained that organisational culture is influenced by the leaders of the organisation, and has the power to shape the success of the organisation. Ndlovu (2020) found that among other things, the success of the organisation in the market is dependent on its organisational and ethical culture.

There are no laws regulating digital ethics or governance in South Africa and many other parts of the world. The King IV Report is the authority on the governance of ethics in South Africa. According to the IoDSA (2016) King IV Report, ethics and corporate governance fall within the ambit of the Social and Ethics Committee (SEC). The King IV Report requires companies to compile codes of conduct and ethical policies. This means that the SEC mandate can be extended to the governance of digital ethics.

As advanced by Li (2023), in no distant future, there might be regulatory developments relating to digital ethics, for the same reason that the Protection of Personal Information Act (POPIA) was created to protect data privacy. This view is reinforced by the fact that the affordance and advancement accorded by digital technologies cannot be abandoned because of the harm they cause to society. At this stage, the only mechanism available to protect society is self-regulation by individual organisations. This self-regulation can be enhanced by organisational digital ethics guidelines and industry specific guidelines (Li, 2023), while other scholars believe that industry

targeted regulations or blanket one size fits all regulations are required (Schiff et al., 2020).

Some of the digital technologies end up creating harm because of misuse, poor design, poor development, lack of technical skills, lack of quality assurance, and incorrect application (Winfield et al., 2019; Eitel-Porter, 2021), algorithm bias and lack of system audit trail to enable transparency (Schiff et al., 2020). The governance of ethics should be properly executed to address all the said problems.

The failure of governance can have a negative impact on the continuing existence of an organisation (Ndlovu, 2020). The failure of governance has directly or indirectly caused some of the world known corporate scandals like Enron, WorldCom, Parmalat, Lehman brothers, and others (Stubben & Welch, 2018). Some of these companies ceased to exist because of those scandals. South Africa also has its own fair share of scandals caused by lack or weak governance. The point in this case includes Steinhoff, VBS, Eskom, and others. Some of these governance failures were laid bare at the Judicial Commission of Inquiry into Allegations of State Capture, Corruption, and Fraud in the Public Sector including Organs of State, headed by Judge Raymond Zondo (Zondo Commission). The sustainability of these organisations was substantially affected, resulting in financial losses, reputational damage, and job losses.

The failures of governance of digital ethics also have consequences. According to Eitel-Porter (2021), the consequences can include reputational damage, which depending on the extent thereof can cause financial loss and negative customer experience. The other consequences are non-compliance to laws or governance standards, in the South African context which might include King IV (governance of ethics) and POPIA (data privacy). The third consequence mentioned by Eitel-Porter (2021) relates to making incorrect decisions based on incorrect data or poorly designed systems. Eitel-Porter (2021) submits that in an organisation with negative ethical culture, one of the consequences of governance of digital ethics is that employees will not report failures of governance of digital ethics.

2.4.3 *Requirements of digital ethics governance*

There is no difference between the governance of digital ethics and that of conventional corporate ethics, however, organisations should strive to make a distinction between the two, by reviewing the existing policies and procedures (Schiff et al., 2020). Eitel-Porter (2021) advocates for the use of existing ethics governance structures, rather than creating new ones, to avoid creating duplications and competing forums. In addition, the existence of two ethics governance structures (one for digital ethics and another for corporate ethics) might create confusion for employees (Eitel-Porter, 2021).

Stahl (2022) suggested that the governance of digital ethics should include the appointment of an AI or Digital Ethics Officer (DEO) or any overall accountable authority and the appointment of the Digital Ethics Governance Committee (DEGC). The DEO must have technical and ethics knowledge and must be the custodian of the digital ethics framework (DEF) (Stahl, 2022). The DEO must chair the DEGC committee. Stahl (2022) cautioned that as much as the DEO is the custodian of digital ethics, the responsibility of enforcing digital ethics should be of everyone in the organisation. Therefore, there must be deliberate efforts to quell the perception that the DEO is solely responsible for digital ethics.

The appointed DEGC members should be senior employees who have the technical and business knowledge, and the necessary authority to make decisions (Blackman & Ammanath, 2022). The management of digital ethics must be handled by the DEGC under the chairpersonship of the DEO. The SEC must be updated on the workings of the DEGC. The SEC is an equivalent of the Ethics Board as suggested by Eitel-Porter (2021). The DEGC must consist of several role players (Becker et al., 2022) and it must be multidisciplinary (Winfield et al., 2019; Eitel-Porter, 2021). The people with technical and non-technical skills should be appointed are technologists, legal, ethics, and business experts (Blackman & Ammanath, 2022). Those with technical skills are those involved in the design and creation of digital solutions, and the non-technical skills are those who use or manage the effectiveness of digital solutions like business operations, risk, and ethics (Stahl, 2022; Mišić, 2021; Winfred et al., 2019). The other non-technical people can be added to the DEGC depending on the unique circumstances of the organisation.

The ethics and risk professionals must address the ethics and reputational risks concerns; the technical professionals must assess the suitability of the technology to be deployed; the legal professional must assess issues of compliance and legal issues; and business professionals must assess the viability of the digital solution on the business operations (Blackman & Ammanath, 2022). The governance of digital ethics is essentially a risk management process. This means risk management processes should be embedded from the initiation until post implementation of the digital technologies. The DEGC among other things, must conduct or ensure that the impact analysis is conducted, which should include regulatory impact; individual and society impact; and financial and economic impact of the implementation of the digital technologies and solutions (Ashok et al., 2022). Eitel-Porter (2021) suggested that the following should form part of the governance of digital ethics:

1. Determining the founding principles or guidelines: Those that could be adopted are reflected in Table 2 and Table 3. The selection of the guidelines must be influenced by the type of industry in which the organisation operates and the values of the organisation.
2. Establish the Ethics Board (SEC): Depending on the size of the organisation, there could be a separate committee relating to this. The JSE listed companies and other types of companies that must comply with King IV must have SEC.
3. Establish the DEGC: The structure must deal with how digital ethics decisions would be made and documented. It is best to use existing structures that employees are familiar with, rather than starting new ones. The members should be from diverse backgrounds and should execute their functions based on a framework.
4. Organisational wide training: The training must be tailor-made for various levels of employees. For example, senior employees should attend training that empowers them to set the tone at the top. The employees must be trained on the importance of digital ethics and the processes involved in managing the governance of digital ethics.
5. Digital ethics metrics: It should detail how digital ethics would be measured, including the tools and mechanisms that will be employed.

6. Foster dissent: Those who serve on the DEGC must have authority and be able to express themselves if there are people acting outside of the digital ethics framework. The important feature of this is that the committee must be multidisciplinary to avoid unconscious bias.

2.4.4 *Proposition 1*

Organisations practice digital ethics governance to prevent harm to stakeholders; and to protect the organisation from the consequences of failure of governance, non-compliance to laws, reputational damage, and financial loss.

2.5 Digital ethics framework

The governance of ethics should be executed based on a framework that is anchored by the selected guidelines, the values of the organisation, and other considerations. The DEF must be robust and be able to withstand varying circumstances of digital ethics (Becker et al., 2022)

2.5.1 *Definition*

Since 2016, there has been an increase in the research focussed on guidelines of digital ethics (Winfield et al., 2019; Schiff et al., 2020). An example of some of these digital ethics guidelines include human rights, privacy, autonomy, fairness, justice, and others. In addition to those mentioned in Table 2, various digital ethics research outcomes produce overlapping outcomes and terminologies (Floridi & Cowls, 2019). The various research papers have referred to these guidelines as tenets, values, and principles of digital ethics (Floridi & Cowls, 2019).

In this research report the tenets, values, principles, and frameworks, are referred to as guidelines. This includes those in Table 2 who were referred by Jobin et al. (2019), Armstrong and Lee (2022), and Ashok et al. (2022) as digital implications, principles, and harms of digitisations. The analysis of the guidelines mentioned in Table 2, was chosen for this research report because they were recent. The oldest was developed by Jobin et al. (2019) four years ago. There are no universal digital ethics guidelines, Eitel-Porter (2021) suggested that each organisation must adopt its guidelines based

on the type of industry they are in and the values of the organisation. A similar suggestion was made by Becker et al. (2022), who indicated that due to the number of guidelines available, each organisation must select what suit its own set of circumstances, and use that to create its own DEF.

2.5.2 *Digital ethics guidelines*

Jobin et al. (2019) conducted a study of 84 digital ethics guidelines from across the world, and they found that there are five common emerging principles, and they are transparency, justice, fairness, non-maleficence, responsibility, and privacy. Ashok et al. (2022) conducted a study of 59 research articles on digital ethics, relating to eight ethical research domains in digital transformation covering four domains of digital ethics, which are physical, cognitive, information, and governance. The said study led to the identification of 14 digital ethics implications linked to the said domains. Armstrong and Lee (2022) identified 10 harms or consequences harms of digitisation. The five common principles identified by Jobin et al. (2019), the 14 digital ethics implications identified by Ashok et al. (2022), and the 10 harms of Armstrong and Lee (2022) are reflected in Table 2.

The analysis of the said guidelines was based on the four domains of digital ethics. For example, in the physical domain, Ashok et al. (2022) identified dignity and well-being, safety and sustainability; while Jobin et al. (2019) identified non-malfeasance; and Armstrong and Lee (2022) identified physical well-being and emotional or psychological well-being. According to (Floridi & Cowls, 2019) non-malfeasance means no harm, overuse, or abuse of digital technologies. The three researchers identified similar concerns relating to the physical domain.

Table 2: Digital ethics principles, implications and harms

Ashok et al. (2022) digital ethics domain	**Ashok et Ashok et al. (2022) Digital implications**	**Jobin et al. (2019) principles of digitisation**	**Armstrong and Lee (2022) harms of digitisation**
Physical	• Dignity and well being • Safety • Sustainability	• Non-maleficence	• Harms to physical well-being • Harms to emotional or psychological well-being
Cognitive	• Intelligibility • Accountability • Promoting prosperity • Fairness • Solidarity • Autonomy	• Fairness • Responsibility • Justice	• Harm to fairness • Harm to transparency • Harm to Autonomy • Harm to trust • Threat to justice • Harms to emotional or psychological well-being
Information	• Privacy • Security	• Privacy	• Harm to privacy • Harm to identity
Governance	• Regulatory impact • Individual and societal impact • Financial and economic impact		

There were overlaps in the cognitive domain for the three researchers. For example, Jobin et al. (2019) and Armstrong and Lee (2022) identified justice in this domain, while Ashok et al. (2022) did not. All three identified fairness in their guidelines. The key

guidelines relating to the cognitive domain were fairness, autonomy, justice, and no emotional and psychological harm. In the information domain, privacy was the common denominator for all three researchers. Ashok et al. (2022) and Armstrong and Lee (2022) identified security and identity respectively. In the governance domain, only Jobin et al. (2019) contributed, the other two scholars did not.

The analysis indicated that Ashok et al. (2022) guidelines are much more granular than the other two. On the governance domain, it went a step further to cater for regulatory impact, individual and societal impact, and financial and economic impact, which all fall under the governance domain. These are critical in this study because they directly impact the victims of digital fraud. The overall analysis of the guidelines reflected in Table 2, resulted in the identification of consolidated digital ethics guidelines based on the common denominators. As such, consolidated guidelines are reflected in Table 3.

Table 3: The consolidated digital ethics guidelines

Ashok et al. (2022) digital ethics domain	**Common denominators**
Physical	• No physical harm or compromise of safety
Cognitive	• Fairness • Autonomy • Justice • No emotional or psychological harm
Information	• Privacy
Governance	• Regulatory impact • Individual and societal impact • Financial and economic impact

2.5.3 *Digital ethics framework*

The digital ethics guidelines are useful but are not enough to mitigate against the harm created by digital technologies or digital solutions. The usefulness of digital ethics guidelines can be augmented. According to Mišić (2021), the guidelines need to be

refined to suit the day to day application. Otherwise, they remain vague guidelines that do not empower those who must apply them. Beyond the guidelines, a DEF must include details about the assessment, design, and use of digital technologies within the organisation (Mišić, 2021). Stahl (2022) refers to this as an impact assessment process and Winfield et al. (2019) refer to this as ethical risk assessment. The DEGC must satisfy themselves that the impact or ethical risk assessment and all the elements of the DEF have been addressed prior to approving the use of the digital technology or solution.

According to Mišić (2021), the DEF must have a requirement for a need analysis to be conducted. That is the evaluation of the need to create a digital solution. The analysis of the need must be supported by evidence, which can include trend analysis, scenario-based analysis, and so forth. Once that is completed, the risk of the proposed digital solution must also be evaluated. The design of the digital solution must then consider the insights obtained during the assessment, which should include mitigating the identified risks (Winfield et al., 2019). Prior to implementation the digital solution must be tested, and if it does not yield desired results, it must be fixed before it is implemented (Winfield et al., 2019). Armstrong and Lee (2022) refer to the impact assessment as a social cost benefit analysis, which seeks to ascertain whether the implementation of the technology or solution is warranted, or whether the need can be fulfilled without the digital technology or solution. Some of the considerations in this case could be whether automation should be implemented if it will lead to job losses, especially where the benefits of automation are equal to keeping the same employees on the job. This impact assessment ensures that digital technologies are not applied at all costs without considering the available alternatives.

Post implementation of the digital technology or solution, there must be continuous monitoring to test whether it is functioning as intended, and that it yields the desired results. The testing must be holistic, that is, both the positives (opportunities) and negatives (risks) must be checked. The functioning of the digital technology or solution must be transparent, and this can be made possible by having an audit trail (Winfield et al., 2019; Eitel-Porter, 2021). The availability of the audit trial allows for monitoring to ascertain whether the technology or solution is working as intended. Armstrong and Lee (2022) identified elements in their digital ethics comprehensive framework. Some

of those elements were also researched by other researchers as indicated below. The elements are as follows:

Element 1: The importance of risk management identified by Mišić (2021).

Element 2: Ethical design identified by IEEE (2017).

Element 3: The isolation of responsibility (the appointment of the DEO) identified by Stahl (2022).

Element 4: The adoption of founding principles of guidelines (adoption of hypernorms and micronorms) identified by Eitel-Porter (2021).

Element 5: Compliance with laws (if they exist) by Floridi (2018), Stahl (2022), and Li (2023).

Element 6: The social cost benefit; or regulatory, individual, societal, financial, and economic impact as identified by Ashok et al. (2022); or Digital ethics or risk impact assessment as indicated by Winfield et al. (2019).

The other elements identified by Armstrong and Lee (2022) relate to protecting and regulating access to digital assets (Element 7), which relates to cyber security. However, the protection of digital assets does not only include cyber security, they also require physical protection which has not been catered for by Armstrong and Lee (2022). The reality is that digital assets can be digitally and physically harmed or attacked. The literature review also identified other elements of the digital ethics framework in addition to the mentioned eight elements. The additional elements are as follows:

Element 8: The digital technologies and solutions should have an audit trail as indicated by Winfield et al. (2019) and Eitel-Porter (2021).

Element 9: Post implementation monitoring as indicated by Winfield et al. (2019)

A consolidated digital ethics framework based on the literature review conducted is reflected in Figure 2.

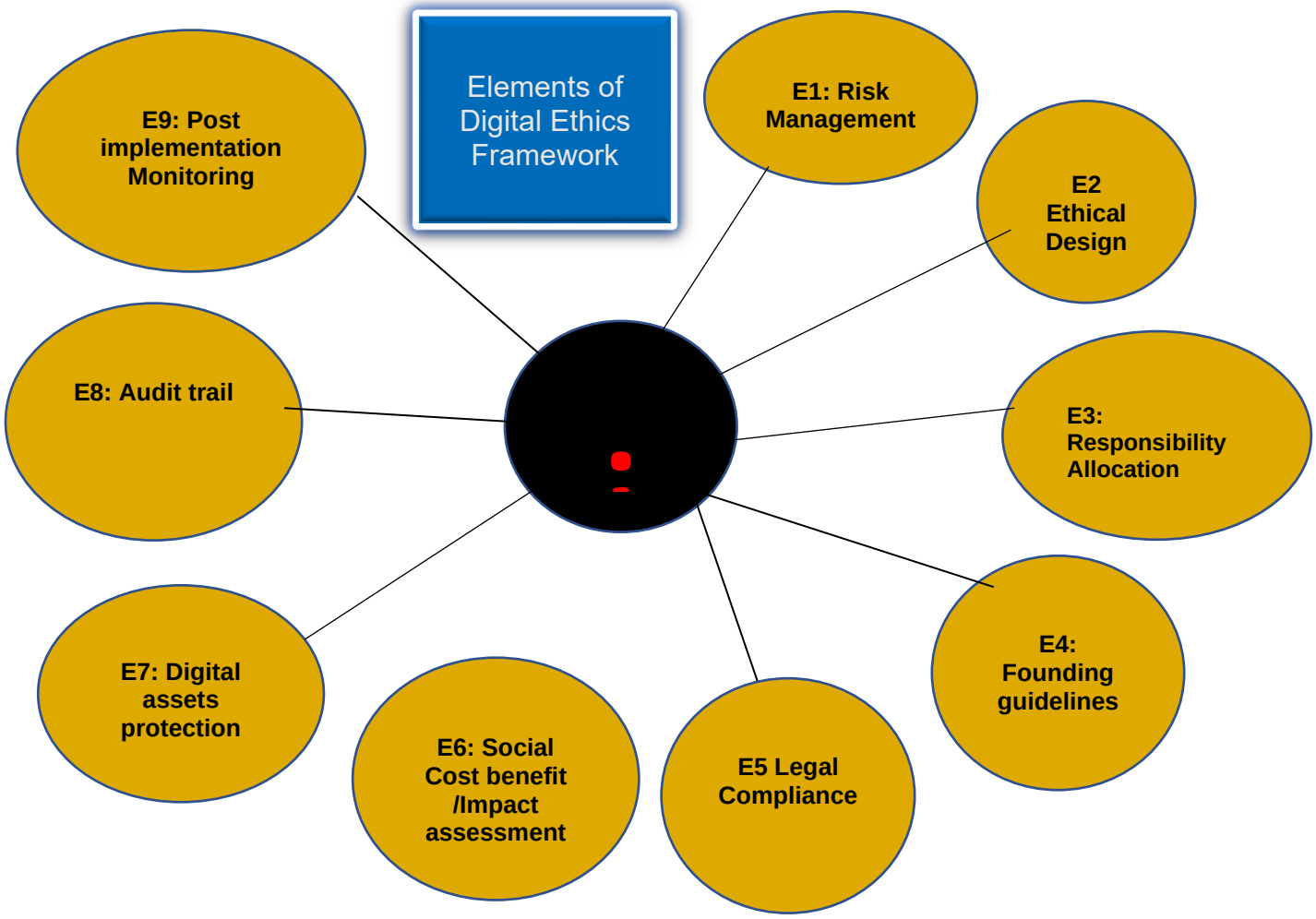

Figure 2: Consolidated digital ethics framework

2.5.4 *Proposition 2*

A digital ethics framework includes risk management, ethical design, responsibility allocation, founding guidelines, legal compliance, impact assessment, digital asset protection, audit trail, and post implementation monitoring.

2.6 The digital fraud risk management

Digitalisation is enabled by the internet. Without the internet, there would not be social media, online shopping, online banking, online learning, and other conveniences like working from home (WfH). Conversely, the internet is also an enabler of digital fraud and other forms of ills in cyber space. Digital fraud is the most common crime in the

digital era (Kemp, 2020; Cavaliere et al., 2021) and it affects millions of people (Batra et al., 2020). Fraud is hampering the wide adoption of e-commerce platforms by customers (Cavaliere et al., 2021). The prevalent digital fraud is spamming, phishing, malware, and identity theft (Khadas, 2020; Batra et al. 2020). Other types are retail fraud, mobile network enabled banking fraud like interception of OTP (sim-swap and porting fraud) with the view of gaining unauthorised access to the victim's bank account; and others like credit card fraud (Batra et al., 2020). The other types of digital fraud identified are application fraud, account takeover, money mules, and profile building (Graydon, 2020). All these types of fraud occur in the digital space which is made possible by the internet.

There are numerous ways in which fraudsters can breach and penetrate the cyber security defences of the organisation to commit fraud. The causes thereof include the non-use of strong passwords and failure to patch systems, which then allow irregular access to the network (Khadas, 2020). The sharing of passwords among employees and the non-removal of resigned employees from the organisational systems fall in that category. There is no correlation between the amount spent on digital protection, including cyber security, and the extent of digital fraud or cybercrime experienced by the organisation (Buil-Gil et al., 2021). However, the investment in that regard is not fruitless because it contributes to protecting the organisation from being overly exposed to digital fraud and cybercrime in general (Buil-Gil et al., 2021). The more digital touchpoints the organisation has, the higher chances of being victims of digital fraud (Buil-Gil et al., 2021).

Fraud can be either perpetrated by any stakeholder of the organisation (Ahmad et al., 2020). These stakeholders might be internal or external to the organisation. The internal stakeholders include employees, trade unions, partners, and service providers. The internal stakeholders, according to Fourie (2019), perpetrate internal fraud, which is segmented into employee fraud and management fraud. The external stakeholders primarily include mainly customers and general members of the public (Ahmad et al., 2020), but also include investors, regulators, and others. In other instances, digital fraud is committed by organised crime groupings consisting of internal and external

stakeholders (Ahmad et al., 2020). According to Mostafa (2022), these groupings are well funded and highly incentivised for their efforts. Internal fraud is prevented by organisation emanating controls and can detected through various methods including whistleblowing (Graydon, 2020). Marzuki et al. (2020) mentioned that the greater attention to preventing fraud should be focused internally because this is where most of the fraud is committed. The effective defence against externally perpetrated digital fraud is prevention, and not law enforcement authorities because ordinarily they handle a minimal amount of fraud committed in organisations (Graydon, 2020).

2.6.1 *The causes of digital fraud*

There are various causes of digital fraud in an organisation. Some of those causes are a weak control environment and a lack of tools, processes, and skills to prevent and detect fraud. Most importantly, the amount of fraud perpetrated is dependent on the ethical culture, and the higher the ethical culture, the less incident of fraud (Ndlovu, 2020; Cavaliere et al., 2021). Therefore, it means the positive ethical culture is a non-negotiable deterrent that serves as a bulwark against fraud and any ills that can affect the organisation. The board and senior management are responsible for creating the ethical culture, and for ensuring that the control environment is effective to prevent fraud (Fourie, 2019). To achieve that, Fraud Risk Management (FRM) practices should be embedded in the organisational culture (Marzuki et al., 2020).

According to Bezuidenhoud and Geldenhuys (2019) and Fourie (2019), the creation of the said positive ethical climate is dependent on the correct leadership tone and organisational values. Erin et al. (2021) found that there is a positive relationship between effective practices of risk management and the reduction of digital fraud. They also found that sound risk governance improves the performance of the organisation. The absence of a positive ethical culture, weak governance, and internal controls creates a fertile ground for reprehensible conduct in an organisation.

The existence of a positive ethical culture does not completely insulate the organisation from internal and external fraudsters. One of the reasons for that is that the organisation does not exist in isolation from the broader society. The socio-economic levels of the country or the environment in which the organisations operate also contribute to the levels of fraud. The high levels of unemployment and poverty

contribute to the commission of digital fraud (Batra et al., 2020). Compounding the situation is that the person's propensity to commit crime is also influenced by the culture of that particular society (Fourie, 2019). This is also worsened by a lack of consequences for those who commit acts of cybercrimes, including digital fraud (Babanina et al., 2021). The contributing reason for that is the under reporting of these incidents to law enforcement agencies by the victims (Babanina et al., 2021).

The internet has enabled the globalisation of digital trade and digital fraud. Digital fraud is pervasive because it is not confined by geographical constraints (Pasculli, 2020). Due to the anonymity and non-physicality of digital fraud, it can be committed in multiple jurisdictions by the same actors (Babanina et al., 2021). These types of fraud are perpetrated with sophistication, speed, and precision (Detura et al., 2022), and this is one of the contributors for the fraudsters going unpunished for their criminal deeds. The sophistication of digital fraud is not always related to the fraudster’s high-technical skills, the socio economic factors and the available opportunities that can be exploited are also contributor as indicated by Batra et al. (2020).

Despite the increase in the sophistication of the commission of digital fraud, organisations, customers, and society in general, cannot afford to stay away from digital technologies because they are an integral feature of everyday living (Mostafa, 2022). The irreplaceable nature of the internet and the convenience it affords, are the reasons that the digital space remains a conducive environment for many harms, including digital fraud. Instead of reporting the incidents to the law enforcement authorities, the victims of digital fraud choose to disassociate themselves from organisations linked to the crime, because of the perception that the perpetrator would not be apprehended (Yonder, 2023). It has become the survival of the fittest for organisations and individuals. Each and every organisation fights its digital fraud battles silently, there is no industry coordination, and the beneficiary of out of this is the fraudsters (Mostafa, 2022). In South Africa, this picture might change because the Cybercrimes Act (2020) imposes reporting obligations on organisations to report certain types of cybercrime.

The Information and Communication Technology (ICT) organisations of which MNOs are part, are the most victims of cybercrimes compared to other industries, and this could be because of the perceived values of these organisations (Buil-Gil et al., 2021). The pursuit of digital transformation must not cause organisations to neglect the creation of positive ethical culture and effective FRM practices. According to Marzuki et al. (2020), FRM consists of fraud identification, evaluation, prevention, and monitoring. Digital transformation also enables sophisticated types of digital fraud, and this must elevate the importance of FRM, to ensure there are no trade-offs between digital transformation and the prevention and detection of fraud (Detura et al., 2022). In that case, there is a responsibility on organisations not to contribute to the increase of digital fraud, by only focussing on the upside of digital technologies and solutions, by neglecting the risks.

2.6.2 *The risks of digital fraud*

The impact of digital fraud on an organisation has been under researched, but the limited research conducted indicates that the private sector specifically spends a lot of money on preventing themselves from being victims (Buil-Gil et al., 2021). Crime in general, digital or not, has dire consequences for organisations and society in general. According to Abubakari (2021), Detura et al. (2022), Graydon (2020), and Mostafa (2022) the impact of digital fraud on organisations are as follows:

1. Reduction of customers' trust in the digital systems and digital touchpoints.
2. Reputational damage due to negative publicity.
3. Financial loss for the organisation.
4. Negative customer experience.
5. Erosion of the ethical culture.
6. Reduce investor confidence.
7. Non-compliance with certain laws (for example POPIA).
8. Loss of sensitive business information.
9. Business disruption.

2.6.3 *The mitigation of digital fraud*

The prevention of digital fraud must be driven from a higher level of the organisation, and it must executed based on the FRM plan or strategy (Graydon, 2020). According to Graydon (2020), the organisation must galvanise its stakeholders to be the first line of defence against any attacks meted out by fraudsters; this can only happen if there are heightened levels of ethics and fraud awareness training within the organisation. According to Graydon (2020) ethics and fraud awareness training must be augmented by other interventions like regular data back-ups and other measures.

The training must be extended to service providers and other internal stakeholders especially if they have access to the organisation network. Buil-Gil et al. (2021) indicated that organisation that prioritises ethics and fraud awareness training suffer less incidence of digital fraud and cybercrime in general. The awareness of digital fraud must be provided to customers and the members of the public, and this could be in the form of warnings and digital fraud trends prevailing in the industry at that specific time (Yonder, 2023). Transparency rather than opacity helps customers and the public to be informed about digital fraud (Yonder, 2023).

Graydon (2020) argued that the prevention and the mitigation of fraud start and end with the organisation; the organisation cannot look for answers elsewhere other than themselves. There are several ways in which digital fraud can be mitigated, these include having a robust authentication process to validate the customers and employees (Detura et al., 2022). The latter is key, especially for the organisation that has employees that are WfH. Buil-Gil et al. (2021) found that organisations that does not allow employees to Bring Your Own Devices (BOYD), reported high incidences of email fraud, this is because the organisations have mechanisms to detect the said fraud. Buil-Gil et al. (2021) opined that this detection is high because if the fraudulent emails had been directed at employees' devices, they would have not been detected. Mostafa (2022) indicated that conducting official business on mobile devices, social media and removable devices like Universal Serial Bus (USB), should if possible be prohibited, based on the risks that they pose.

Batra et al. (2020) is of the view that the normal advice of having strong passwords, secure systems, and networks can be improved with the adoption of digital technologies like ML and data analytics. ML, data mining, link analysis, and other analysis can be used to react to different types of digital fraud scenarios (Ahmad et al., 2020). Data analytics is effective in identifying trends and patterns, which can trigger an alert to management or functions tasks with fraud examination to review the transactions (Ahmad et al., 2020). The fraud data analytics must be configured to generate exception reports once red flags have been identified. There should be clear roles as to who is responsible for acting on the said red flags (Graydon, 2020). Continuous fraud risk assessments should be conducted, including software programs that can prevent and detect fraud should be considered (Graydon, 2020). Organisations that invest in building internal capabilities to address cybercrimes, respond much better to cybercrime much better than organisations that primarily rely on outsourced capability (Buil-Gil et al., 2021).

2.6.4 *Proposition 3*

The mitigators of digital fraud include a positive ethical culture, sound governance, effective FRM practices, and responsible use of digital technologies.

2.7 ANALYTICAL FRAMEWORK

The analytical framework addressed both the theoretical framework and the conceptual framework.

2.7.1 *Theoretical Framework*

The study proposes the stakeholder theory as the theory that underpins this study. This is because the stakeholder theory requires that the organisation balances the interest of the organisation’s stakeholders (Alsayegh et al., 2020). Li et al. (2021) indicated that organisations must be guided by the dictates of the stakeholder theory to ensure that it does harm its stakeholders. Relating to the proposed study, the stakeholder theory would ensure that there is a balance between the application of digital technologies and the risks of digital fraud. Both these initiatives must equally be

prioritised, to ensure that there is no harm to stakeholders, specifically customers and members of the public in this case.

Detura et al. (2022) argued that digital technologies must be managed to ensure that they yield positives that will propel the organisation to succeed in the market, but equally, the risks that cause unintended consequences must also be managed. According to Armstrong and Lee (2022), the stakeholder theory also places a legal duty on management to comply with the laws and responsible corporate citizenship commitments, which include issues of digital fraud. Armstrong and Lee (2022) posit that the stakeholder theory places an ethical obligation on management to ensure the survival of the firm to the benefit of all stakeholders. This includes ensuring that the organisations avoid harms like digital fraud which might threaten the survival of the organisation and negatively impact stakeholders.

As much as technology has agency, Martinho et al. (2021) argued that digital technologies cannot have moral agency because it does not have freedom and cannot be held responsible. No matter how smart or advanced the technology is, those who use them must be held solely responsible (Hallamaa & Kalliokoski, 2020). The stakeholder theory focuses on stakeholder relationships, because that is the basis for the existence of the organisation (Freeman et al., 2021). One of how the harm can be mitigated is sharing of information with the stakeholders. The transparency by the organisation enables trust, legitimacy, and good reputation (Alsayegh et al., 2020). This transparency includes sharing the details about how the organisation is governed, including the governance of digital ethics and digital fraud. Li et al. (2021) indicated that concepts like Environmental, Sustainability, and Governance (ESG) draw inspiration from concepts like stakeholder theory, and by extension, any organisation that adopts ESG is in a way embracing stakeholder theory. Organisations that embeds stakeholders theory perform better than their peers (Li et al., 2021).

The stakeholder theory's covers areas like strategy management, corporate governance, business ethics, and others (Freeman et al., 2021; Valentinov and Chia, 2021). The importance of this theory was demonstrated by the 2019 "Statement of Corporate Purpose" made by 181 CEOs of major organisations, who committed to

managing their organisations for the benefit of all stakeholders (Freeman et al., 2021). The application of the stakeholder theory is conducive to the turbulent environment (Valentinov, 2022). The imperatives to digitise have been imposed and accelerated by various factors, including COVID 19. Based on that reason, it can be argued that the organisations currently operate in a turbulent environment.

Organisations strive to be successful in the market, it is for that reason that there is a bias towards consideration for opportunities and neglect of risks. Valentinov (2022) posits that stakeholder theory mitigates that specific risk because it considers the interest of all stakeholders, and not just the creation or betterment of the competitive advantage. The theory achieves this by ensuring that there are sound relationships between the organisation and the stakeholders it serves (Freeman et al., 2021). There must be a cultivation of win-win relationships between the organisation and various competing interests of stakeholders (Valentinov & Chia, 2022). This can be achieved if there is proper governance of ethics that will prevent harm to stakeholders.

There is evidence from other scholars that the proper application of stakeholder theory can increase the performance of the organisation; and that there is no contradiction between the creation of competitive advantage and the stakeholder theory (Freeman et al., 2021; Li et al., 2021). This can be achieved if the pursuit of profit and success does not occur at all costs, to the detriment of stakeholders. The theory will be impacted if the adoption of digital technologies enhances the competitiveness of the firm but increases digital fraud because of poor digital ethics practices.

2.7.2 *Conceptual Framework*

The conceptual framework is influenced by two key concepts of the study, that is, digital ethics and digital fraud. It was influenced by the literature review, which found that organisations must practice digital ethics governance to prevent harm to stakeholders and to protect the organisation from the consequences of failure of governance; that the digital ethics framework must be robust and comprehensive; and that positive ethical culture, governance, and FRM practices are primary conditions to deal with digital fraud. Lastly, the conceptual framework was influenced by the stakeholder theory which was adopted for the study. The stakeholder theory emphasises that organisations should balance the interest of stakeholders, which means there must be

equal management of both the opportunities and risks. The conceptual framework is illustrated in Figure 3.

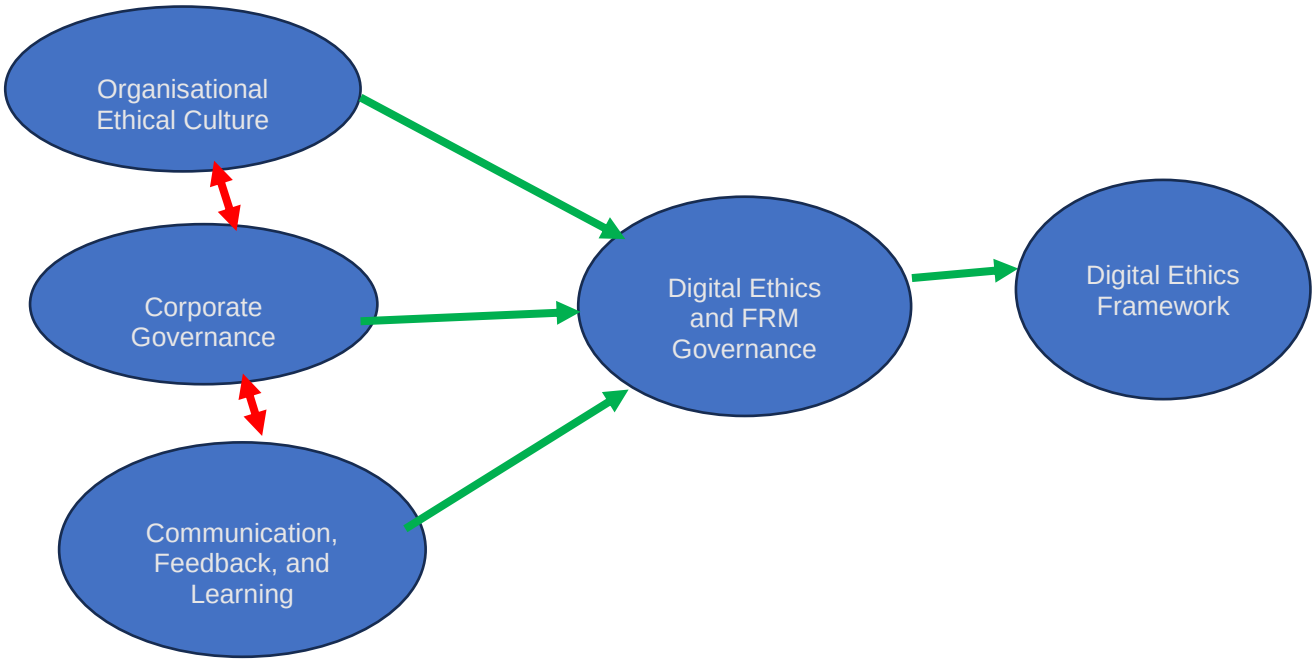

Figure 3: Conceptual framework

Figure 3 indicates that organisational ethical culture is foundational to any organisation, and a positive ethical culture will enable a conducive environment for effective corporate governance (Ndlovu, 2020). Among other things, the ethical culture is enabled by the correct leadership tone and organisational values (Bezuidenhout and Geldenhuys, 2019; Fourie, 2019). The positive ethical culture enables the practice of corporate governance and vice-versa as denoted by a double-headed arrow. Among others this includes SEC having oversight on how ethics is governed within the organisation.

As advocated by the stakeholder theory, to act in the interest of stakeholders, the organisation must communicate, receive feedback and learn from those engagements. This to and from is also denoted by the double-headed arrow. The ethical culture, corporate governance, and communication, feedback, and learning create a fertile environment for the effective governance of digital ethics and FRM. All these will allow

for the development and/or implementation of the comprehensive digital ethics framework indicated in Figure 2.

2.8 Conclusion of Literature Review

The literature review indicates that digital ethics should not be treated as an afterthought. It should be embedded in the way ethics is governed in the organisation to ensure that the risks of digital technologies are mitigated. This must be performed to protect the organisation and stakeholders, and to increase the chances of success in the market. Through the literature review, the following three propositions were identified.

2.8.1 *Proposition 1*

Organisations practice digital ethics governance to prevent harm to stakeholders; and to protect the organisation from the consequences of failure of governance, non-compliance to laws, reputational damage, and financial loss.

2.8.2 *Proposition 2*

The digital ethics framework must include risk management, ethical design, responsibility allocation, founding guidelines, legal compliance, impact assessment, digital asset protection, audit trail, and post implementation monitoring.

2.8.3 *Proposition 3*

The mitigators of digital fraud include a positive ethical culture, sound governance, effective FRM practices, and responsible use of digital technologies.

CHAPTER 3. RESEARCH METHODOLOGY

This chapter details how the research was conducted. It explains the research methodology that was followed and the reasons for selecting them, this includes the research approach, the research design and sampling method, the research instrument, ethical considerations, study limitations, quality assurance, and the data analysis techniques that will be employed. The qualitative research design was used, this was influenced by the research objectives, research questions, and the insights obtained from the literature review.

3.1 Research approach

The study adopted an exploratory approach to explore the application of digital ethics practices to mitigate digital fraud in an MNO in South Africa. The research was empirical because it collected raw data and it contributed to the generation of new knowledge (Dan, 2017). The research took on an interpretivism paradigm by being an exploratory and qualitative study. The Interpretivism paradigm research is qualitative, socially constructed, has multiple meanings, focuses on narratives and interpretations, has small samples, yet has detailed investigations (Saunders et al., 2019).

The exploratory research was chosen because it is suitable when a new or unknown phenomenon is being investigated (Singh, 2021), as is the case of the application of digital ethics practices to mitigate digital fraud. The primary data collection method used was semi-structured interviews. The qualitative research design was adopted because it allows the participants to share innate and extensive context based on their experiences and insights (Jackson et al., 2007), and how they view a particular issue (Elkatawneh, 2016). The study used the inductive approach because it allows theory to develop from the raw data by deriving concepts and themes (Thomas, 2006). The inductive studies are necessary for theory development (Saunders et al., 2019).

3.2 Research design

The types of qualitative research designs are historical, case study, action research, phenomenological, ethnographic, and grounded theory. A qualitative research was chosen because it is thorough, and it is appropriate to answer research questions that ask “how” and “why”; where the researcher has no influence on the research problem (Cleland, 2017). A qualitative research study allows for a deeper understanding of participants' experiences, which cannot be explained quantitively. The qualitative study engages participants in their natural settings, and they reveal complex and rich sets of findings compared to quantitative studies (Cleland, 2017). Aspers and Corte (2019) mentioned that the following are the advantages and disadvantages of qualitative design:

Advantages:

1. They study people or things in their natural settings, and the outcome is based on the meanings provided by the participants.
2. They reveal nuances that are hidden behind the quantitative numbers, they get closer to the actual truth than the quantitative design.
3. They collect data based on various empirical methods like interviews, documents, observation, personal experiences, life stories, and others.

Disadvantages:

1. They are not scientific because they use words rather than numbers, and thus they are subjective. However, according to Aspers and Corte (2019), other scholars have refuted this disadvantage by indicating that the data collected through the qualitative design is much more reliable and provides deeper insights than the data collected via a quantitative design.

3.3 Data collection methods

The data was collected using semi-structured interviews with Company X management level employees involved with the application of digital technologies, products or

solutions, digital ethics, and digital fraud. According to Ruslin et al. (2022), semi-structured interviews are suitable for exploratory research because they allow a deeper understanding of a phenomenon. Unlike structured interviews, semi-structured interviews are flexible and allow additional questions to be asked based on the responses from participants (Ruslin et al., 2022). The interview guide was used as the primary data collection method. It was designed based on the three prepositions formulated in Chapter 2. The interview guide was reviewed by the academic supervisor to ensure that it addresses the research questions. This data collection method was suitable to respond to the research questions.

3.4 Population and sample

This section details the population and the sampling procedure that was undertaken during the study.

3.4.1 *Population*

A population is a group of people who are the subjects of the study (Shukla, 2020). According to Shukla (2020), the population of the research must be well defined. The target population of the study consists of management level employees of the incumbent organisation taken from the functions that manage the implementation of digital technologies, products or solutions, digital fraud, and digital ethics. Any person outside of that parameter was excluded from the population.

3.4.1 *Sample and sampling method*

A sample is a selection of a certain representation from the defined population (Gentles et al., 2015; Ishak & AbuBakar, 2014). A sample is a sub-set or a part of the population and it represents the population in which it was chosen (Shukla, 2020). The participants were selected based on non-probability purposive sampling which provides a greater understanding of the study (Ishak & AbuBakar, 2014). Purposive sampling also allows the researcher to select different types of participants, who will better respond to the

research questions and provide a detailed understanding of the phenomena being investigated (Gentles et al., 2015; Ishak & AbuBakar, 2014).

The participants were selected according to their management level status, and most importantly because of their involvement in the implementation of digital technologies, products or solutions, digital fraud, and digital ethics. Due to its sheer size, it is not always possible to subject the entire population to the study. In that case, sampling becomes critical because it saves time and financial resources (Shukla, 2020). The purposive sampling was essential because it allowed the selection of suitable participants that responded to the research questions. The purposive sampling method provides deeper insights irrespective of whether they are representative of the population (Gentles et al., 2015).

The management level employees involved in digital technologies, products or solutions, digital fraud, and digital ethics were selected. They were selected because of their knowledge and involvement in the said sections or functions. As reflected in Table 4, all 12 management level employees were interviewed. A qualitative research is not about obtaining a representation of the population, but it is about the depth of the information collected from the participants (Staller, 2021). The 12 management level employees are from three diverse functions. According to Ishak and AbuBakar (2014), a sample that is selected from diverse participants enhances the study because it eliminates bias, and provides an opportunity to obtain a diverse and rich context.

Table 4: The sampling of participants

Functions	**Number of management-level employees**
Digital Technologies (Products)	2
Digital Fraud	2
IT (Digital Ethics)	3
ERM & Ethics	2
IS	3
Total	**12**

3.5 The research instrument

The development of the interview guide was influenced by the literature review that was conducted, as reflected in Chapter 2. The interview guide was prepared for the face to face or virtual semi-structured interviews. The interview guide is attached as Annexure A. The interview guide was explained to the participants. The interview guide contained open-ended questions to obtain deeper context about the phenomenon. There were follow up questions that were asked to the participants (Kallio et al., 2016).

As indicated above, the interview guide was reviewed by the academic supervisor to ensure that it yielded the required data from the participants. All this was necessary because a properly designed and tested interview guide enhanced the trustworthiness, credibility, confirmability, and dependability of the study (Kallio et al., 2016). The interview guide included the factors illustrated in Table 5. The interview guide contained the main concepts or themes of the study as well as questions that must be asked under that theme or concept (Kallio et al., 2016).

A previously used interview guide relating to a similar study was not found. As a result, the interview guide was developed from scratch. The interview guide was segmented into the three research questions, and the actual questions asked were influenced by the three propositions of the study, the theoretical and conceptual framework.

Table 5: The factors influencing the interview guide questions.

Research questions	**Propositions**	**Theoretical framework**	**Conceptual framework**
Research question 1 How is governance of digital ethics practiced in	**Proposition 1:** Organisations should practice digital ethics governance to prevent harm to stakeholders; and to protect the organisation from the consequences of failure of governance, non-compliance to laws,	The stakeholder theory requires that the organisation balances the interest of the organisation's stakeholders	The conceptual framework is indicated in Figure 3. <u>In summary:</u> The conceptual framework indicates that firstly a positive ethical culture

Company X?	reputational damage, and financial loss.	(Alsayegh et al., 2020). Li et al. (2021) indicated that stakeholder theory ensures that there is no harm to stakeholders. The theory will ensure there is a balance between the application of digital technologies and solutions and the risks of fraud. Both initiatives must be equally prioritised Detura et al. (2022)	is enabled by the correct leadership tone and organisational values. Secondly, there must be corporate governance. Thirdly, there must be governance of digital ethics and FRM. Lastly, there must be a comprehensive and robust ethics digital framework. The arrows on the left and right denote the application of stakeholder theory. The arrows indicate communication flowing from inside and outside the organisation.
Research question 2 What are the components of the digital ethics framework in Company X?	**Proposition 2:** The digital ethics framework must be robust and comprehensive; it should include risk management, ethical design, responsibility allocation, founding guidelines, legal compliance, impact assessment, digital asset protection, audit trail, and post implementation monitoring.		
Research question 3 How are the risks and causes of digital fraud mitigated in Company X?	**Proposition 3:** A positive ethical culture, sound governance, and effective FRM practices are primary mitigators of digital fraud; the organisation must not use digital technologies in a manner that causes the risk of digital fraud.		

3.6 Procedure for data collection

The researcher is employed by Company X. As per the permission given to the researcher by the organisation, the participants were approached directly based on their seniority (management level employees) and the extent of their involvement in digital technologies, products or solutions, digital fraud, and digital ethics. Depending on their availability, the participants were approached directly, via face to face, email, or telephone. All 12 interviews were conducted virtually using Microsoft Teams, and

they were recorded and transcribed as agreed with the participants. The duration of the interviews was 60 minutes.

Prior to the commencement of the interviews, participants were provided with the participant information sheet and the participant agreement (consent forms). These documents are attached herein as Annexure B and Annexure C respectively. The participants agreed that the interviews be recorded. The context of the research including the research problem was explained to the participants prior to the commencement of the interviews. This allowed them to ask questions for clarification.

3.7 Data analysis strategies and interpretation

The study used thematic analysis for analysing collected data. The thematic analysis allows for the identification of patterns or themes, and it further allows analysis within those identified themes (Bowen, 2009). According to Braun and Clarke (2012), thematic analysis allows for the identification of shared and unique participants' experiences within a dataset. Thematic analysis is generally used during qualitative research (Braun & Clarke, 2012), this is because it is easy to use and is the most used method of qualitative studies (Braun & Clarke, 2012). Thematic analysis can be used for data collected using semi-structured interviews (Bowen, 2009).

3.8 Possible limitations and challenges of the study

The following are the limitations of the study:

1. The study only focussed on the mitigation of digital fraud, not any type of risks that might be impacted by digital ethics.
2. The study is qualitative research and was confined to the specific Company X context, which might not exist in other MNOs or organisations.
3. Only management level employees were interviewed, the study did not consider the views of top level and bargaining or low-level employees.

3.9 Quality Assurance

The quality assurance in qualitative research includes transferability, credibility, dependability, and confirmability.

3.9.1 *Transferability*

According to Stenfors et al. (2020), transferability means that the study details the context in which the research was conducted and the findings thereof. Most importantly, transferability relates to whether the study can be transferred to another setting (Stenfors et al., 2020). Tracy (2010) indicated that it is difficult for qualitative research to achieve transferability because, unlike quantitative studies, they use non - probability sampling. The study attempted to diminish the sampling hurdles. The following was performed in a manner suggested by Tracy (2010), the research report provides a direct quotation and detailed description of the experiences of participants which can be related by other people to their specific situations outside of the study being studied. The use of purposive sampling also heightened the transferability of the study (Cameron, 2011).

3.9.2 *Credibility*

The credibility of the research is enhanced when justified reasons are provided as to why a particular research methodology was applied (Stenfors et al., 2020). The justification for the methodology chosen is provided above. To enhance credibility, the interview guide was checked for correctness by the academic supervisor (Denzil & Lincoln, 2018; Stenfors et al., 2020). The fact that the interview guide was prepared based on the literature review also enhances the credibility of the study (Denzin & Lincoln, 2018). The researcher works for Company X, to minimise the subjective bias of the researcher, data was not collected from the function or area where the researcher is employed (Denzin & Lincoln, 2018). The alignment between the theory, research question, data collection, analysis, and results ensured that the study was credible (Stenfors et al., 2020).

3.9.3 *Dependability*

According to Stenfors et al. (2020) and Cameron (2011), dependability relates to whether there is sufficient information for the study to be replicated. Sufficient and detailed information is provided to enable another researcher to replicate the steps in a different setting or context (Tracy, 2010). This study was exploratory qualitative research, where data was collected through semi-structured interviews. The dependability of the study is heightened by the fact that the interview guide will be made available to other researchers (Kallio et al., 2016). The study also strived to reach a point of saturation based on the responses received from the participants to enhance dependability (Denzin & Lincoln, 2018).

3.9.4 *Confirmability*

According to Cameron (2011), confirmability relates to the research report fully reflecting the experiences and accounts of the participants. This study obtained an intense understanding of the phenomena being researched within the context of Company X. The research process employed throughout is provided to improve the chances of confirmability (Kallio et al., 2016). The confirmability of the study was heightened because the research process was transparent, all the audit trail from the conceptualisation of the problem, the importance of the study, research questions, literature review, research design, data collection method, and analysis is provided (Denzin & Lincoln, 2018). The researcher was objective to enhance the confirmability of the study (Kallio et al., 2016), it is for that reason that data was not collected from the function or area where the researcher is employed (Denzin & Lincoln, 2018).

3.10 Ethical considerations

According to Halai (2006), qualitative research must address the following ethical considerations: informed and voluntary consent, confidentiality, anonymity of participants, no harm to participants; and reciprocity. Halai (2006) explains that

reciprocity relates to the benefits that the participants derive from participating in the study. Each of the said elements was addressed as follows:

1. Informed and voluntary consent: The purpose of the study was explained to the participants. They were provided with the participant information sheet and the consent form before the commencement of the interview. They were informed that they could revoke their consent during or after the interview had been conducted.
2. Anonymity of the participants: The identity of the participants has not been mentioned in the research report. No other information which makes them identifiable was mentioned in the research report. The participants will be identified as Participant (P)1, P2, P3, P4 and so forth. The participant was also not identified through recorded interviews.
3. Confidentiality: The information shared by participants was not revealed to any party outside the scope of the research.
4. No harm to participants: The compliance with the above points, that is, informed and voluntary consent, anonymity, and confidentiality ensured that there is no harm to participants. No conduct from the researcher caused harm to the participants.
5. Reciprocity: The research participants were not compensated for their participation; however, they will be reciprocated by the knowledge that will be generated from the study.

In addition to the above, the following was conducted to eliminate the ethical concerns:

1. The study was conducted as per the approval or permission received from Company X, which is attached herein as Annexure D.
2. The name of the organisation and any identifiable feature was not mentioned in the report, as per the permission received from Company X.
3. The data collection commenced after the required ethical clearance was received from the university. The ethical clearance is attached as Annexure E.
4. The data collected and all the information relating to the research is housed inside a folder within a laptop computer. The folder and the laptop can only be accessed via a password, and only the researcher knows the password. The laptop password is changed monthly. No person will be provided with the

password of the laptop or folder. Only the researcher and the academic supervisor have access to the data collected during the research.

5. None of the participants reported directly to the researcher, the participants were employed in different divisions of Company X.
6. The final research report was subjected to plagiarism checks, using the Turnitin software, and the relevant declaration forms were signed. The first page of the Turnitin report is attached herein as Annexure F.

CHAPTER 4. PRESENTATION OF FINDINGS

4.1 Introduction

This chapter presents and describes the findings of the study. It starts with providing background details of the participants. The findings were based on the interviews conducted with participants. The analysis was conducted using the thematic qualitative approach as indicated in section 3.7 of this report. The findings are outlined as per the propositions mentioned in Chapter 2.

4.2 Background information

The background information relating to Company X and the participants is indicated below.

4.2.1 *Background on Company X*

The qualitative study was based on Company X, one of the MNOs in South Africa. Company X like most organisations is impacted by digital transformation. The digital transformation has to be undertaken because the MNO industry has been experiencing declining margins due to the increasing cost of doing business. The focus of the study was on mobile network services, specifically relating to the application of digital ethics practices to mitigate digital fraud.

4.2.1 *Background on Participants*

As indicated in Chapter 3, there were 12 participants employed within the various functions of the organisation. The interviews were conducted via Microsoft Teams, they were recorded and transcribed as per the consent received from the participants. As per the approval received for the study, the identity of the participants will not be revealed and thus they will be referred to as P1 to P12.

The relevant details of the participants are indicated in Table 6. The average years of service for the participants of the study was 15 years, which indicates that they had

deep institutional knowledge and experience. Their experience was spread across the practices of digital ethics; they were relatively senior and were managing or leading different functions relevant to the study. They provided deeper insights which allowed detailed findings to be collected. The gender and race distinction between the participants was not done, because it was not necessary. The distinction was also not done because it had the potential of unwittingly revealing the identity of participants.

Table 6: List of participants

Participants	Designation	Years of service	Section
P1	Manager: Enterprise Architecture	6 years	IT (Digital Ethics)
P2	Specialist: IT Governance & Risk	7 years	IT (Digital Ethics)
P3	Senior Manager: Information Security & Risk Governance	9 years	Information Security
P4	Specialist: Information Security Assurance	2 years	Information Security
P5	Senior Specialist: Ethics & Governance	28 years	Ethics Office
P6	Senior Manager: Wireless Application Services	10 years	Digital Technologies (Products)
P7	Corporate Unit IT Lead	39 years	IT (Digital Ethics)
P8	Executive: Enterprise Risk Management	10 years	Mobile Finance
P9	Manager: Credit Vetting & Fraud	25 years	Mobile Operations
P10	Specialist: Credit Management	32 years	Mobile Operations
P11	Manager: Information Security & Risk Management	3 years	Information Security
P12	Senior Manager: Prepaid Services	10 years	Digital Technologies (Products)

4.3 Thematic analysis process

A common thread was maintained along the process by ensuring that the analysis was guided by the following research questions:

1) How is governance of digital ethics practiced in Company X?
2) What are the components of the digital ethics framework in Company X?
3) How are the risks and causes of digital fraud mitigated in Company X?

The thematic analysis process was conducted as reflected in Figure 4.

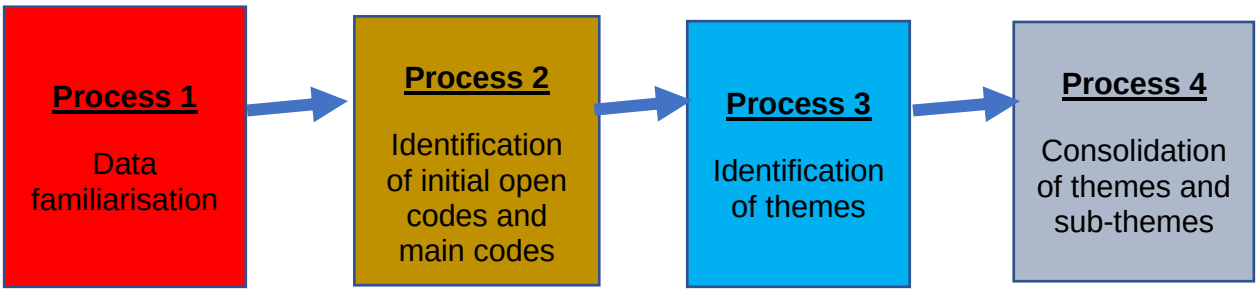

Figure 4: Thematic Analysis Process

4.3.1 *Data Familiarisation*

As indicated, the 12 interviews were recorded and transcribed using Microsoft Teams. Each transcript was read through. The reading was conducted with the above research questions in mind. The data that was not correctly transcribed was fixed. This also included the removal of people's names and the identity of the incumbent organisation where it was mentioned by participants. This was to ensure that the identity of the organisation and the participants were not revealed.

4.3.2 *Identification of open codes and main codes*

The identification of initial open codes and main codes is reflected in Table 7 below. The identification of codes was not pre-determined. The codes were identified as the data was being analysed.

Table 7: Initial Codes

Research Question 1: How is governance of digital ethics practiced in Company X?	Research Question 2: What are the components of the digital ethics framework in Company X?	Research Question 3: How are the risks and causes of digital fraud mitigated in Company X?
Governance 1. No governance of digital ethics 2. Lack of awareness of digital ethics 3. Lack of knowledge of the digital ethics framework 4. IT and IS governance. 5. IT/IS governance will include DE in the future. 6. Conventional corporate ethics governance 7. Business resistance 8. Lack of funds and resources 9. Risk Governance 10. Commercial Review Committee 11. SAP system compliance 12. Digital strategy not aligned with digital ethics framework.	**Product and Solution testing** 1. Digital solutions are tested by IT before implementation. 2. Testing is not done from the digital ethics perspective. 3. Ethics is not involved pre or post implementation testing. 4. Fraud team is not involved in the design of new products and solutions. 5. Future involvement of the Fraud team in the design of new products 6. Vulnerability management is performed. 7. Management of end-of-life devices 8. IS conducts its own tests when a digital system or tools are acquired. 9. IS conducts using its security checklist. 10. Testing of digital solutions or designs does not involve other functions. 11. During Change Request other functions are represented	**DE Risks and Challenges** 1. IT/IS Risk Register is not specific to digital ethics 2. No governance of digital ethics 3. No compliance with the digital ethics framework 4. No measurement or monitoring of digital ethics 5. No tracking of misuse algorithm bias, poor design, and others 6. Immature digital ethics practices 7. Resistance to change 8. No other digital ethics components in the framework 9. Segregation of duties 10. Access governance failures 11. Disposal of information 12. Access review improvements 13. Improved password management 14. Subscription fraud 15. Application and Identity fraud 16. Risk transfer to third-parties 17. No checks of algorithm bias 18. Digital strategy not aligned to digital ethics framework 19. No mechanisms to check prejudices or harm to the customer 20. No post implementation reviews of digital 21. Training and awareness to reskill employees 22. No involvement of diverse functions
Reporting and membership 1. SEC deals with conventional corporate ethics, and not digital ethics. 2. ITEB is responsible for IT governance and digital ethics 3. ITEB reports to the IT Starring Committee (ISC) 4. ISC reports to the Governance & Risk Committee and Board Risk Committee 5. ITEB and ISC focus on IT/IS and not digital ethics. 6. ITEB is Heads of IT and IS 7. ISC is GCEO, GCFO, CIO, BU CEO, IT Leads, and Risk 8. SEC approved digital ethics framework. 9. Reporting to RC every quarter, reporting to SEC situational	**Diverse background** 1. No single forum for diverse functions 2. No end-to-end review of digital risks by diverse functions 3. Digital ethics activities are functionally based 4. The most involved functions are IT and IS 5. Least involved functions Ethics, Fraud and Risk 6. Security checklist	**DE Practices** 1. Biometrics, double-opt in, OTP, Debi-check, AVS 2. Supplier compliance, clawbacks, and termination of contracts 3. Report to the police and civil proceedings 4. Rules for sending/not sending customer messages 5. Third parties: produce evidence that consent was granted by the customer. 6. Third parties: Commit not to abuse customer data 7. First debit order failure investigation 8. Strong authentication process, no virtual sim-swap 9. Strict 3rd party management measures 10. Facial recognition (in progress) 11. Access to the Home Affairs database 12. Access removal of delinquent agents 13. Targeted communication and awareness to employees and customers.
Organisational Culture 1. Conservative organisational culture 2. Resistance to change 3. Change Management 4. Training and awareness	**Authentication** 1. Active directory 2. Multi-factor authentication 3. Access reviews 4. Virtual Private network	

5. SAP declarations 6. New ways of communicating 7. Tone at the top 8. Consequence management 9. Scorecard 10. Loss recoveries	5. Endpoint security 6. Perimeter and network security 7. User access governance. 8. Vulnerability management 9. Third-party security and data protection 10. Sharing of logging credentials 11. Failure to remove former employee access credentials 12. Incorrect user profiles 13. Ineffective password change process 14. System improvements: access log-in 15. Exception reports	14. Red flags analysis every 2 hours to identify fraud. 15. Manual checks while the Change Request is in progress. 16. Digital fraud decreased due to biometrics, AVS, debi-check, and OTP. 17. Designs of products and solutions are done with fraud in mind. 18. Supplier code of conduct 19. System improvements: Change Requests 20. Digital password protected invoices. 21. Acceptable user (IT) policy 22. GRAFT measure and monitor system abuse and fraud 23. Penetration and vulnerability tests 24. Access governance, data privacy, and data classification standards 25. Software development life cycle, quality assurance, and penetration testing 26. Isolation of responsibility, compliance to POPIA, cybersecurity act, audit trail. 27. Post implementation is done only by IS (and products, separately) 28. The 10 Security domains: 29. Commercial Review Committee 30. Weekly digital steerco 31. Focus on digital transformation 32. Prioritise sales generation and what can harm the customer 33. Six product reviews 34. Robust design phase
Incidence Reporting 1. No specific digital ethics reporting 2. Fraud, Ethics, and IS reporting is available. 3. DE reporting: line management and multiple touchpoints 4. Distinction between conventional corporate ethics and digital ethics 5. DE addressed by ethics, risk, fraud, or internal audit	**Tracking of risks** 1. There is no DE Risk Register 2. Generic register of all risks and IT/IS register is being kept separately 3. There is a continuous risk assessment of digital risks 4. Digital risks are tracked until they are fully mitigated. 5. Digital risks are reported to the ERM Forum, IGRC, and Risk Committee 6. Digital risks software for online exposure.	
	Vulnerable Systems 1. Monitoring of system prone to abuse - showstopper applications. 2. Weekly or daily exception reports 3. Frequent access reviews 4. Consequence management 5. Focus on transactions prone to abuse 6. Physical validation - Fingerprint biometrics 7. OTP	
	Opportunities vs harms 1. No active or deliberate analysis to check that digital solutions cause harm 2. No prioritisation of revenue over harm to customers 3. Every digital tool or solution that is assessed only by IS/IT 4. The Project Steerco maximises digital opportunities and risks 5. Digital fraud prevention and sales generation conflicts 6. Engaged and responsive management 7. Third-party consequence management 8. Continuous improvement to minimise customer harm	
	Incident Communication 1. Awareness of employees and service providers is done but it is not enough 2. Not enough awareness to customers and members of the public. 3. External awareness is only done when there is an absolutely necessary 4. Awareness about issues of DE, scams like phishing and fraud. 5. Digital platforms and SMS messages 6. Third-party leadership engagement on fraud trends	
Research Question 1:	**Research Question 2:**	**Research Question 3:**

The colours reflected in Table 7 denote the following: green is for question 1, yellow is for question 2, and orange is for question 3. The identification of initial open codes and main codes was conducted after the data familiarisation process was completed. The initial open codes were refined after duplicates were removed. The codes were grouped as per the research questions as reflected in Table 8. This process identified 151 initial open codes. The said number can be broken down into 36 initial open codes for question 1, 59 for question 2, and 56 for question 3.

The initial 151 open codes were further refined and classified into 14 main codes, after the identification of patterns in the data. They were classified as reflected in Table 8. The four main codes were for question 1, eight for question 2, and two for question 3.

Table 8: Main codes

Research Question 1:	**Research Question 2:**	**Research Question 3:**
1. Governance 2. Reporting and membership 3. Organisational Culture 4. Incident Reporting	1. Digital Product and Solution testing 2. Diverse background 3. Authentication 4. Tracking of Risks 5. Authentication 6. Vulnerable System 7. Opportunities vs harms 8. Incident Communication	1. Digital ethics risks and challenges 2. Digital ethics practices

4.3.3 *Identification of themes*

Once the identification of initial open codes and main codes was completed, further analysis was performed to identify the main themes per research question and proposition. The themes identified per research question and proposition are indicated from Table 9 to Table 11. Some of the themes identified are the same as the main codes that were identified, and others changed.

Table 9: Identified themes for Proposition 1

Main codes	Proposition	Identified themes
1. Governance 2. Reporting and membership 3. Organisational Culture 4. Incidence Reporting	Organisations should practice digital ethics governance to prevent harm to stakeholders; and to protect the organisation from the consequences of failure of governance, non-compliance to laws, reputational damage, and financial loss.	1. Governance 2. Non-implementation of Digital Ethics Framework 3. Organisational Culture 4. Incidence Reporting

The themes for question 1 and proposition 1 are reflected in Table 9, and they are derived from the main codes indicated in Table 8. There were four main codes, and four themes were identified. The themes are governance, non-implementation of the Digital Ethics Framework (DEF), organisational culture, and incidence reporting.

Table 10: Identified themes for Proposition 2

Main codes	Proposition 2	Identified Themes
1. Product and Solution testing 2. Diverse background 3. Authentication 4. Tracking of risks 5. Vulnerable Systems 6. Opportunities vs harms 7. Incident Communication	The digital ethics framework must be robust and comprehensive; it should include risk management, ethical design, responsibility allocation, founding guidelines, legal compliance, impact assessment, digital asset protection, audit trail, and post implementation monitoring.	1. Risk Management 2. Combined Reviews & Testing 3. Access governance and priority systems management

The themes for question 2 and proposition 2 are reflected in Table 10, and they are derived from the main codes indicated in Table 8. There were seven main codes, and three themes were identified. The themes are risk management, combined review and testing, access Governance, and priority systems management.

Table 11: Identified themes for Proposition 3

Main codes	Proposition 3	Identified Themes
1. Digital ethics risks and challenges 2. Digital ethics practices	A positive ethical culture, sound governance, and effective FRM practices are primary mitigators of digital fraud; the organisation must not use digital technologies in a manner that causes the risk of digital fraud.	1. Digital ethics risks and challenges 2. Digital ethics practices

The themes for question 3 and proposition 3 are as reflected in Table 11, and they are derived from the main codes indicated in Table 8. There were two main codes, which were also identified as the themes. The themes are digital ethics risks and challenges and digital ethics practices.

4.3.4 *Consolidation of themes and sub-themes*

There were 151 initial open codes, further analysis resulted in the identification of patterns in the data and 14 main codes. The 14 main codes were further analysed, and ultimately nine themes were identified as reflected in Table 9 to Table 11. The final themes are consolidated in Table 12 together with their corresponding sub-themes.

Table 12: Consolidated themes and sub-themes

Main themes	Sub-themes
1. Governance	• Current governance • Future governance • Reporting
2. Nonimplementation of DEF	• Resistance to change • Lack of funds and resources • Lack of understanding of digital ethics • Digital strategy not aligned with DEF
3. Organisational Culture	• Negative contributions to organisational culture • Positive contributions to organisational culture • Ethics in general
4. Incidence Reporting	• No dedicated reporting for digital ethics • Distinction between corporate and digital ethics • Digital ethics issues addressed by multiple functions

5. Risk Management	• Tracking of risks • Incident communication • Digital Opportunities vs digital harm
6. Combined Reviews & Testing	• Limited testing of digital solutions • Testing not done from a digital ethics perspective • No combined approach to digital ethics
7. Access governance and priority systems management	• Access governance challenges • Vulnerable systems monitoring
8. Digital ethics risks and challenges	• System and process risks and causes. • Digital fraud risks and causes. • Employee and third-party risks and causes • Strategic and operational risks and causes
9. Digital ethics practices	• System and process mitigation • Digital fraud mitigation • Employee and third-party mitigation • Strategic and operational mitigation

The relationship between the said themes is summarised through a thematic map as reflected in Figure 5.

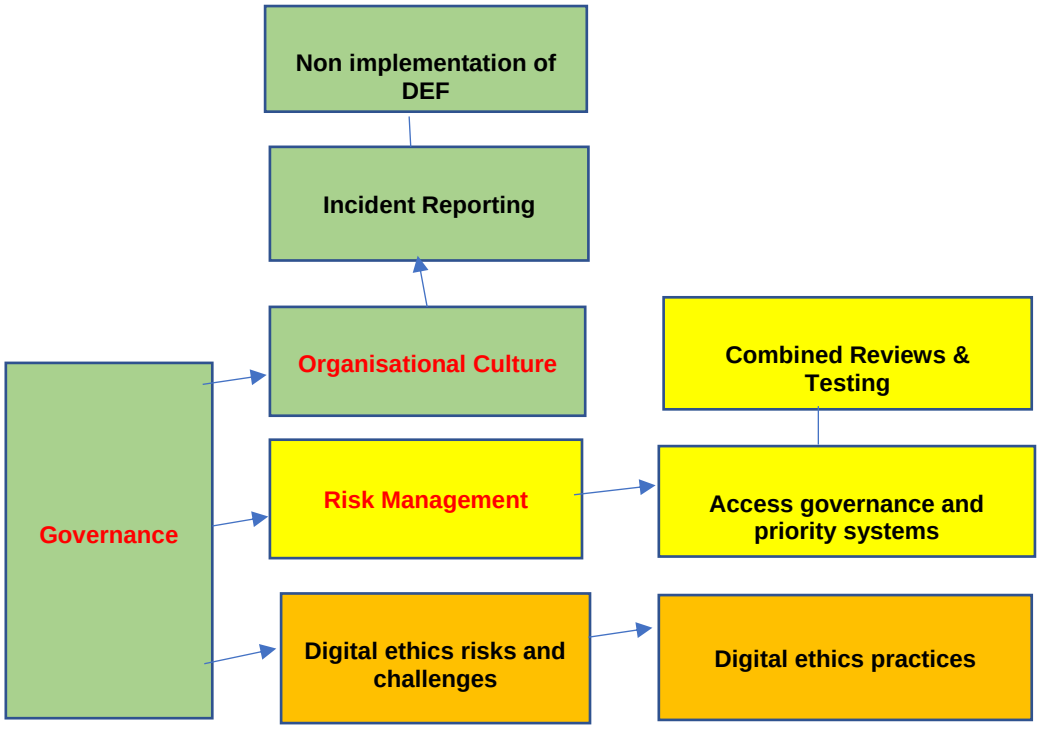

Figure 5: Thematic Map

Figure 5, the thematic map, is depicted in terms of the colours of the research questions and propositions. As indicated above, green denotes question 1 and proposition 1, yellow denotes question 2 and proposition 2, and orange denotes

question 3 and proposition 3. The dominant themes are reflected by the red font (writing), and they are governance, organisational culture, and risk management. The other six remaining themes as reflected in Table 12 are anchored by the three mentioned themes, with governance being the key theme among all those, as it links up with both proposition 2 and proposition 3.

4.4 Results pertaining to Proposition 1

Proposition 1 indicates that: **Organisations should practice digital ethics governance to prevent harm to stakeholders; and to protect the organisation from the consequences of failure of governance, non-compliance to laws, reputational damage, and financial loss.**

The thematic analysis process was used to test this proposition, based on the findings derived from the primary data, which was collected using semi-structured interviews. The results of this proposition are explained below.

4.4.1 *Governance*

The research instrument collected data relating to the governance of digital ethics. The findings were that there is no governance of digital ethics, other than the existence of the DEF. However, it was found that there is proper governance of IT and Information Security (IS). It was found that digital ethics is not governed, and the DEF is not enforced. Digital ethics is not formally practiced and governed by any structure. There is also no Digital Ethics Governance Committee (DEGC).

> *"Digital ethics is not embedded in the governance of ethics"* – P2.

Relating to IT and IS, there is a structure called the IT Executive Board (ITEB), which consists of the Group Chief Information Officer (GCIO), Business Unit Chief Information Officers (BU CIOs), IT Leads, Chief Enterprise Architect Program Manager and relevant specialists. The ITEB is responsible for the IT and IS governance framework. It was found that in theory, the ITEB is also responsible for digital ethics,

but in practice, it is not. The ITEB has not conducted any work relating to digital ethics other than the development of the DEF.

> *"The governance processes are focussed on information security and data management than digital ethics"* – P1.

The work of the ITEB feeds into the IT Steering Committee (ISC), which is made up of Group Executive Committee members of the organisation. The work of ITEB also feeds into the Governance and Risk Committee (GRC), which is responsible for the overall Enterprise Risk Management (ERM). The GRC has more or less the same membership as the ISC. The work of the ISC and the GRC feeds into the Board Risk Committee (RC). There is also a Commercial Review Committee (CRC), which deals with the launch of digital products but does not address digital ethics issues.

> *"The only body that exists is the Commercial Review Committee, but it only looks at issues from a commercial perspective"* – P6.

There was an acknowledgement from participants that digital ethics was not adequately governed within the organisation. There were plans to amend the ISC governance to cater to digital ethics, and the digital ethics work will feed into IGRC and RC. One participant indicated that once the DEF is operationalised, each Business Unit (BU) will have its mechanism to deal with digital ethics, but the DEGC or its equivalent will be responsible for the entire organisation. There was also an acknowledgement that all types of ethics, digitally or not should be handled from the same place.

> *"In future, digital ethics will be explicitly catered in governance documents to make it more pronounced"* – P1.

> *"There are specific processes for the governance of conventional corporate ethics, but nothing for digital ethics"* – P5.

One of the participants mentioned that in terms of reporting to the board sub-committees, as much as the DEF was approved by the SEC, there is an absence of quarterly or periodical reporting to the SEC relating to digital ethics or DEF. The work performed by IT and IS ultimately is reported to the RC and does not include digital ethics. As indicated, there was a view that there should not be a distinction between

corporate ethics and digital ethics and that in the future SEC should be responsible for the overall ethics.

> *"Reporting to SEC is situational, but reporting to RC is every quarter. SEC only deals with ethics as stated in KING IV"* – P5.

4.4.2 *Non-implementation of DEF*

Some of the participants indicated that the DEF was approved by the SEC in February 2023. The DEF is guided by the *"digital ethical principles",* which are Autonomy, Justice, Beneficence, Non-Maleficence, and Transparent. It was also mentioned that the DEF is guided by the following principles Competence; Responsibility; Accountability; Fairness; and Transparency. There was an acknowledgement from almost all participants that the DEF only exists on paper. Among others, it was found that the DEF was developed and approved to ensure that digital products and services are managed and offered in an ethical manner. The views of other participants were that, if implemented, the DEF would ensure compliance with laws and regulations and responsible design and/or development of digital technologies.

> *"There is no monitoring and enforcement of the digital ethics framework. The reasons for that were that there were pushbacks from BUs because digital ethics is a new thing. Coupled with that there is also a lack of funds and resources. Based on that, it was decided that only a framework will be developed now, and it will be implemented at a later stage"* – P1

The views from some of the participants were that the DEF was not implemented because of resistance from the business. This was also influenced by the fact that at some stage the organisation was not adequately performing, and it had to retrench some of its employees. The views of those who were involved in drafting the DEF were that digital ethics was not embraced because the focus was on turning the financial fortunes of the organisation, and digital ethics was not seen as a priority.

"*People were fearful for their jobs, and fearful of digital technologies that it will impact their jobs"* – P2.

The views expressed by one participant was that other than fear of jobs, there was resistance to the adoption of new systems or thinking because they might have a negative impact on productivity. There was also pressure to contain costs, and as a result, not many financial and human resources were made available for the DEF. The other view on why the DEF was not implemented was that digital ethics was a new concept, and not many people knew about it. Compounding the problem was that the DEF was not sufficiently communicated. The consequence of that was not many people knew about its existence.

"I am not aware of the (digital ethics) framework, it was not communicated to us, people that are working in the implementation of the digital strategy" – P11.

"The digital ethics framework is not guiding the digital strategy of the company. Greater awareness of the framework will help guide our work" – P11.

The participants mentioned that the organisation has a digital strategy that focuses on digital transformation. The digital strategy aimed to automate as many processes as possible and make services available online to create a good user experience for customers. It was ascertained that as part of the digital strategy, the organisation had addressed issues relating to risk management, compliance with laws, audit trail, data privacy, cyber security, and so forth. It was found that the DEF was not guiding the implementation of the digital strategy.

Lastly, in addition to the fact that there was no awareness created about the DEF, the other view was that it was not implemented because the internal stakeholder was not taken on board from a change management point of view.

"Change management is critical for driving adoption. If it is not done, then there will be no adoption of digital ethics. Digital ethics is a big concept; it therefore needs serious end to end change management initiatives. This is because digital ethics is broad and diverse" – P7.

4.4.3 *Organisational Culture*

There was consensus from the participants that Company X has formal ethics processes and that there is sufficient oversight on corporate ethics. The organisation has an ethics handbook that covers ethical values, declaration of gifts, conflict of interests, fraud, corruption, and whistleblowing. The organisation also has an ESG program. The participant from the Ethics Office indicated that there are ethical compliance requirements on the SAP system, however, there is nothing related to digital ethics. There are practices within the incumbent organisation that have a positive contribution to the organisational culture. The participants mentioned that there are relatively good ethics and fraud awareness and training initiatives, positive leadership tone, and consequence management against those that act outside the values of the organisation.

> *"Management is setting the correct tone and they address risks that are facing the company"* – P5.

> *"There is consequence management for those that misbehave. There are legal or HR proceedings against external and internal people that have caused harm to the organisation"* – P8.

> *"Where progress is lacking on the implementation of recommendations, ERM does follow up with management. Management performance is tracked in terms of the scorecard, which includes the fact that management must implement Internal Auditing and Forensics recommendations"* – P8.

According to most participants, the organisation has zero tolerance towards unethical conduct and fraud. It was mentioned that this is done to enhance the ethical culture. The consequence management that is meted out to delinquent stakeholders includes the following:

a) Financial loss recoveries: These are recovered from employees, service providers, and other parties.

b) Supplier Disciplinary Committee (SDC): The decision can include suspension of a service provider, contract termination and/or in-house blacklisting.
c) Employee disciplinary: The decision can include a warning, dismissal, and/or listing on the in-house blacklisting.
d) Criminal cases: They are opened against any party that has committed fraud or any acts of crime against the organisation. The cases are followed up with the police and prosecutorial services.

According to most participants, there are also practices within the organisation that contribute negatively to the organisational culture. Some of the participants mentioned that the organisational culture is conservative and there is resistance to change. The resistance to change is influenced by the factors indicated in 4.4.2 above. It was found that changes that are made are not accompanied by sufficient change management to ensure employees' buy-in. As much as there are ethics and fraud awareness and training activities, some indicated that they are not impactful, because they are mostly performed virtually and via corporate communications emails. The other issue raised was that the DEF was approved, and yet no training was performed relating to it. The other participants indicated that ethics and fraud awareness and training for third parties must be improved because most of the digital fraud emanates from that environment.

> *"…enhance the organisation culture, through information security, awareness and training and other types of awareness. Where some of training and awareness are compulsory, and those that do not comply are escalated"* – P2.

> *"We need to improve how we manage third parties. The training and awareness on digital ethics must be extended to third parties, especially in areas like call centres which are outsourced"* – P8.

Relating to consequence management, one participant was not convinced that the available measures were sufficient. The participant indicated that there is no transparency around consequence management, and the voice coming from management regarding digital fraud was not strong and consistent. Others indicated that as much the levels of conflict of interest and gift declarations were high on the SAP system, there is a concern that people do not fully disclose their interests as required by the ethics handbook.

4.4.4 *Conclusion on proposition 1*

There is no digital ethics governance within Company X, this conclusion is supported by the views of almost all participants. As a result, there is a risk that there might be harm to stakeholders. The digital strategy is not anchored by the DEF, and consequently, there is a risk of not sufficiently mitigating digital fraud, financial loss, and non-compliance with data privacy laws. Most of the respondents were of the view that the organisational culture is positive, but that was threatened by the lack of governance of digital ethics and implementation of the DEF.

4.5 Results pertaining to Proposition 2

Proposition 2 indicates that: **The digital ethics framework must be robust and comprehensive; it should include risk management, ethical design, responsibility allocation, founding guidelines, legal compliance, impact assessment, digital asset protection, audit trail, and post implementation monitoring**.

The thematic analysis process was used to test this proposition, based on the findings derived from the primary data, which was collected using semi-structured interviews. The results of this proposition are explained below.

4.5.1 *Risk Management*

The views of all the participants were that there is no specific digital ethics risk register, however, there are detailed risk registers for IT, IS, and other business risks facing the organisation. There is continuous risk assessment and digital risks are tracked until they are mitigated. The management of risk feeds into the ERM forum, GRC, and RC. A participant indicated that there are also various software tools to manage cyber security risks. When the risks are identified, a proper risk management process is followed.

There were varying views from participants relating to whether incidences of digital fraud are sufficiently communicated to stakeholders, internally and externally to the organisation.

> *"Internally, people are kept informed. Externally, when there is a need"* – P3.

> *"As much as awareness is done, it is mostly directed at internal people, and not customers or members of the public. Awareness of external people needs improvement"* – P5.

> *"Employees and other internal stakeholders are constantly informed, and customers and members of the public are informed when it is necessary. Some of the issues need to be contained, they are not for public consumption"* – P7.

> *"We are not doing enough to keep employees, service providers, customers, and the public informed about the incidence of digital fraud"* – P9.

> *"We have programs where we communicate with our stakeholders: employees, service providers, customers, members of the public: we send SMS to customers so that they are aware of various issues, including fraud schemes"* – P12.

Based on the dominant views, the communication on digital fraud must improve both internally and externally. The issue of incident communication is closely linked to ethics and fraud awareness and training discussed above. One participant indicated that cyber security awareness among employees was deficient. The impact of that was most of the cyber security digital fraud incidences were caused by a lack of awareness or ignorance of employees. Other views were that every quarter, the fraud team has meetings with leaders from the call centres and store environments to notify them about fraud trends that have been identified and how they can be alleviated. Where there is a need, the fraud trends are communicated as they happen, without waiting for the quarter to end.

It was revealed that the organisation does not have a formal process to assess whether the digital products or solutions do not cause harm to customers. The DEF covers this, but it is not enforced as indicated above. As much as the management of that risk was

not formalised, some of the participants indicated that it was done, but not within the auspices of digital ethics. The views expressed were that management ensures that where digital initiatives cause harm, the problems are fixed. Some indicated that the assessments were conducted, but they were only conducted from an IT and IS perspective. One participant indicated that the assessments were not effective because they were reactive instead of being proactive.

> *"Every tool that is brought in is assessed, its upside and the downside, but that assessment is done by Information security and IT. It is not by a diverse team"* – P3.

> *"If there is harm to customers, we intervene. We don't only prioritise revenue generation. There are at times conflicts between fraud prevention and sales generation. In one instance after the engagement with the salespeople, a correct decision was taken, because that specific product was prone to fraud. Some changes were made to mitigate the fraud. Management listened, and the problem was fixed"* – P9.

> *"Despite revenues coming in, when customers are impacted by the fraud, we act. For example, if we found that a partner was subscribing to customers without their knowledge, we intervened. To mitigate against that, we have introduced a mechanism like a double-opt-in. We tighten controls and if it means that we block the partner* (cancel the contract)*, we do that"* – P12.

The organisation has the Project Steering Committee (PSC), which according to some participants is responsible for maximising digitisation opportunities and the risks emanating from those opportunities. This is done as part of the digital strategy. The participants indicated that the PSC does not include all other relevant functions, and the focus thereof is not digital ethics, even though some elements of digital ethics are practiced.

4.5.2 *Combined Reviews and Testing*

The findings obtained indicate that there is limited testing of digital products and solutions prior to them being used. These digital technologies are mainly tested by IT and/or IS prior to implementation to ensure that they do not weaken internal controls. The post implementation and other activities like penetration testing are performed by IS. The participants mentioned that other functions like ethics, fraud, and others are not involved when digital products or solutions are designed, and during the pre or post implementation tests. Some of the participants acknowledged that there are challenges relating to the involvement of other functions. They indicated that this challenge must be fixed by ensuring that all relevant functions are included as a standard practice.

> *"Digital solutions are tested before they are implemented, but not from the digital ethics point of view. The testing is related to information security, and they check general compatibility and cyber security risks"* – P7.

Some of the participants argued that other functions, but not all, are included when a Change Request (CR) or when User Requirements Specification (URS) is under consideration. Others insisted that even during a CR or URS, it is only IT and IS that are predominantly involved. One view was that the non-involvement of the diverse functions to deal with testing, conceptualisation, and design of digital technologies is also reflected in the composition of the PSC. The other view was that some functions are invited to the PSC on a need to use basis.

> *"Risk* (ERM) *only gets involved at the Project Steerco* (PSC)*, when there is a compliance element to what is being discussed at that time. The regulatory team is only engaged on that basis"* – P8.

A view expressed by a participant from digital products was that the post implementation assessment is only performed by the digital products team. Other functions like IS, IT, and ERM are invited when it is necessary. However, the Revenue Assurance and Fraud Management (RAFM) team is always involved in that process because they are responsible for detecting fraud and revenue loss once digital products are launched.

> *"A function like Revenue Assurance and Fraud Management is always there, but not other teams like fraud and ethics. Perhaps it is things that we have overlooked. At times we have information Security, IT, and Risk. Revenue Assurance and Fraud Management is always invited because they pick anomalies and notify management"* – P12.

There was an acknowledgement from some of the participants that the design and testing would be enriched if performed from a combined point of view.

> *"In the future, the diverse functions should be sitting in a single forum, instead of doing things separately. Doing so is helpful. After all, we will not be coming up with a solution that will not bite us because our view was one dimensional"* – P11.

4.5.3 *Access governance and priority systems management*

Most of the views obtained were that there are several processes relating to access governance. These included users being registered on Active Directory (AD), Multi-Factor Authentication (MFA), access control for different applications, and regular access reviews, amongst others. There is also a Virtual Private Network (VPN) as an added layer when accessing the organisational network. The views of the participants were that besides access governance the following are some of the controls within the incumbent organisation: endpoint security, IS training and awareness; perimeter and network security; vulnerability system management; third-party security; and data protection.

It was mentioned that managers also have a responsibility to check whether their direct reports have the correct profiles. Every month managers receive an automated email with the list of their direct reports. They are required to approve or reject the type of access or profile that their direct reports have. According to the participants, there are mechanisms to ensure that the right person has the right profile. This is achieved by having regular access reviews to avoid employees and third-party employees having access profiles that they do not need, which might be abused to create fraudulent transactions.

Despite all these controls, most respondents indicated that access governance was a challenge. At the centre of those challenges was the sharing of log-in credentials; non-removal of user credentials of those who have left the employ of the organisation; and non-updating of user profiles for employees that have changed roles or moved to other departments. Some of the participants indicated that these challenges result in the profiles being abused to create unauthorised transactions and fraud.

> *"Our biggest problem is that agents still share their username and passwords"* – P9.

One participant indicated that the process of changing passwords is weak. It was mentioned that it was easy for someone to call the call centre and change the logging credentials of their colleague, or a person that has resigned. This is because what is required by the IT Help Desk when a password is changed is the name, surname, contact details, and ID number. A perpetrator armed with these details, can call the IT Help Desk and change the password of their colleague. The person would then be provided a new password and advised to change the password thereafter. Due to digital fraud that has been perpetrated recently, controls were introduced to improve the user authentication process. The controls introduced were related to network log-in and the systems or application log-in.

> *"In the sales environment, especially call centres and shops, the control introduced is that the network log-in details and the system log-in details must be the same. This was introduced after some users logged in to the network by using the credentials of someone, else and then logged into another system and create fraud transactions. Coupled with MFA, it is now difficult for someone to log in to the network using someone's credentials"* – P10.

There are also mechanisms to monitor that key or vulnerable systems are not abused. This is critical in minimizing digital fraud and other nefarious activities. The participants mentioned that one of those is the periodical exception reports that are monitored by IT and RAFT.

"There is a process to monitor the critical systems, we call them showstopper applications. If those applications are affected, then the business is hugely impacted" – P11.

The participants indicated that any anomalies identified by IT and RAFT are then forwarded to management or forensics for investigation. It was mentioned that where there is substantive evidence of wrongdoing, there is consequence management against the implicated parties.

"Sharing of logging credentials is a problem, those that are found there is consequence management" – P7.

The participants from digital fraud indicated that one of the transactions that are vulnerable to abuse is sim-swap. To counter the fraud, a control was introduced, wherein a sim-swap transaction was only allowed to be performed physically at the Store, where the customer could be authenticated by fingerprint biometrics. It was mentioned that sim-swap fraud was reduced because of this control, which was found to be more effective than the OTP control.

4.5.4 *Conclusion on proposition 2*

This proposition indicated that the DEF must be robust and comprehensive. In the case of Company X, this was not the case because the DEF was not enforced. In terms of the proposition, the DEF must include risk management, ethical design, responsibility allocation, founding guidelines, legal compliance, impact assessment, digital asset protection, audit trail, and post implementation monitoring. It was established that not all these aspects are practiced, and even to those that are practiced, some weaknesses need to be improved. The digital strategy is not anchored by the DEF, and because of that, there is a risk that digital fraud might not sufficiently mitigate financial loss, reputational damage, and non-compliance to POPIA. Most of the respondents were of the view that the organisational culture is positive and that the factors that need to be improved are the governance of digital ethics and the implementation of DEF.

4.6 Results pertaining to Proposition 3

Proposition 3 indicates that **A positive ethical culture, sound governance, and effective FRM practices are primary mitigators of digital fraud; the organisation must not use digital technologies in a manner that causes the risk of digital fraud.**

The thematic analysis process was used to test this proposition, based on the findings derived from the primary data, which was collected using semi-structured interviews. The results of this proposition are explained below.

4.6.1 *Digital ethics risks and challenges*

The views expressed by participants relating to this theme were divided into four. This was as follows: systems and processes risks and causes; digital fraud risks and causes; employee and third-party risks and causes; and strategic and operational risks and causes.

Some of the participants indicated that the risks and causes relating to systems and processes were access management issues and lack of segregation of duties. The latter was regarding some of the transactions not having a creator and approver. For example, the transactions were created by an Agent at the call centre or stores, and they were automatically approved by the system because they were below a certain monetary threshold. The views expressed were that this had the potential of being abused because the users knew that the approval would not be executed by a manager.

The other system and process risks indicated were the lack of distraction or disposal of information, and access governance and password management, as indicated above. The latter is exacerbated by the sharing of logging credentials among agents at the call centre and stores.

> *"The process of changing passwords is not rigid enough. It is easy for someone to call the call centre and change the logging credentials of their colleague. To change the password, other than the name, surname, and contact details you just need an ID number only".* – P10.

The other risk highlighted was digital fraud. One of the participants highlighted the prevalence of subscription fraud, which presents itself in different shapes and forms. One of those includes identity fraud, where a victim's details are used to apply for a post-paid mobile account. It was mentioned that subscription fraud can be perpetrated by internal actors, external actors, or both types of actors acting for a common purpose.

> *"Customers' identity is stolen, and fraudsters call the call centre, and apply for credit using the victims' details"* – P9.

> *"I am dealing with subscription fraud, where a person is being impersonated. This is another form of identity fraud. There are different scenarios and a lot of crime syndicates at work. The main aim of this is to open mobile accounts fraudulently, with no intention of making a payment. The company would lose both the mobile device and the revenue"* – P9.

Another scenario reflected concerning subscription fraud was that fraudsters would after opening bank accounts, create some activity in that bank account for three months. This is to create an impression that the banking activities are legit. After three months, the bank statement would reflect salaries or income being deposited and expenses or payments coming out of the bank account. At that stage, the bank account is ripe to be used for fraud. The fraudsters would make a post-paid credit application for a high-end mobile device, of which some cost in excess of R30 000. Once approved, payment will not be made to Company X.

The other risk highlighted by the majority of the participants was that some employees were seeing compliance as a hindrance to their productivity, and they believed that they were entitled to access all systems or information. Others reflected that there is no proper contract management of third parties, which exposes the organisation to POPIA non-compliance.

> *"We need to improve how we manage third parties. The training and awareness on digital ethics must be extended to third parties, especially in areas like call centres that are outsourced* – P7.

"The contracting process must be improved. Part of the solution starts during the procurement process to ensure that subject matter experts from IT and other functions are involved, to ensure that risks are properly transferred to third parties. In these days of POPIA, there needs to be closed monitoring of third parties. For example, partners must not use customer data for other purposes outside the contract" – P8.

There were varying views concerning strategic and operational risks and causes. Some indicated that the main challenges were insufficient, or non-existence monitoring of digital ethics risks related to data privacy and misuse of algorithms.

"Digital ethics practices are not mature" – P1.

"The design phase does not test or check that there is no algorithm bias" – P6.

"Consideration of algorithm bias is not a focus for the company. But it should, since we are considering facial recognition solutions, there should not be facial features bias embedded in that tool" – P11.

Most of the views of the participants were that the practices of digital ethics were not uniformed, and structured. They indicated that this was primarily because of the non-implementation of the DEF. Others highlighted the fact that the ethics function was not involved in the development of the DEF and that the training and awareness of digital ethics were not conducted. They highlighted that training and awareness were a vital driver in the re-skilling of the workforce. Others mentioned that the practice of pre and post implementation tests is situational, it is not a standard practice that is performed for all digital initiatives.

"No checking of digital products and solutions from a digital ethics perspective before they are released. There is no forum that does quality assurance to check all that – P2.

4.6.2 *Digital Ethics Practices*

As was the case with the previous theme, the views expressed were divided into four. This was as follows: systems and processes risks and causes; digital fraud risks and causes; employee and third-party risks and causes; and strategic and operational risks and causes.

The systems and processes risks and causes indicated in the preceding theme are mitigated by some of the digital ethics practices. The participants highlighted that albeit not mature and formal, there was some alignment between digital ethics and conventional corporate ethics. The organisation has an IT acceptable use policy, which details the dos and don'ts. The participants indicated that IS and IT perform numerous checks, including vulnerability checks. There are processes available to monitor systems that are susceptible to abuse. For example, the customer system is being monitored for abuse or manipulation by RAFT and other functions. RAFT and other relevant functions monitor transactions that are of high value and volume. These checks are conducted 24 hours a day.

> *"We constantly check that application controls work as intended and that they are not breached. We also ensure that all machines have the necessary anti-virus systems and so forth"* – P3.

> *"To ensure that we are not exposed, we keep on making sure that we scan our digital services or web facing applications for vulnerabilities. Now and then do penetration test just to make sure that the digital applications are secured"* – P4.

The views of most participants were that there is a raft of controls employed by Company X to protect its customers and other stakeholders from digital fraud. Some of those controls are as follows:

a) The double opt in control was introduced for content or subscription services (Apple, Google, and Huawei services) as an extra protection for unauthorised charges to customers.

b) The OTP control was introduced in the App Stores. The customer must reject or accept a payment via an OTP before the transaction is completed.
c) The third-party consequence management: Where a third party has misbehaved, the loss amount is recovered, a criminal case is opened, and the disciplinary hearing is held in terms of the supplier code of conduct. Third-party contracts are terminated if there are gross violations, and where warranted civil actions are also initiated.
d) There are rules for third parties, which detail when a message can be sent to a customer, and when it cannot be sent. The customers who opt not to receive messages; are removed from the list of messages that are sent to customers.
e) The charging of customers: The customer is charged what was advertised so that the customer knows the costs beforehand.
f) There are exception reports that are generated to check that application systems are not abused.
g) The first payment: Once there is non-payment on the first debit order, the fraud team investigates to ascertain that the failure was not because of application fraud.
h) The post-paid accounts are subjected to a debi-check control to curb identity fraud. The customer must activate a debit-check as a condition for credit approval. The debi-check must be approved by the customer on a cell phone that is registered with the bank.
i) There is also an Account Verification System (AVS), to check that the bank account belongs to the customers. This is to avoid fraudsters using a victim's bank account during the application process.
j) There is a process to block all system access for third-party users that have committed misconduct or fraud within the organisation.
k) There is targeted communication and awareness of fraud trends to various stakeholders.
l) There is an internal blacklisting process, where all parties that have committed misconduct or fraud against the organisation are listed.

One of the participants indicated that exception reports are vital controls to curb digital fraud. There is a report every two hours to identify fraud and non-compliance to the credit vetting process and other policies. One of those is issuing and canceling orders

report, which is checked with a magnifying glass, because of the fraud that was recently uncovered. The fraud was caused by the credit vetting that was not conducted properly, and the fraudulent increase of customer credit limits. There were other incidences where items were added to customers' accounts, without them knowing. It was mentioned that these incidents caused the organisation to lose substantial revenue because the fraudsters were targeting high-end Samsung and iPhone devices.

It was indicated that these mentioned controls are not perfect, but they have helped reduce or eliminate some of the prevalent digital fraud, thus further enhancing the control environment of the organisation.

> *"The subscription fraud has decreased a lot because of fingerprint biometrics as well as AVS, debi-check, and OTP"* – P10.

> *"We ensure that consumers are protected and not harmed by digital services. We do this by creating awareness internally and to customers, about digital scams, including phishing. We don't mail invoices anymore, invoices are now digitized, and encrypted and the code to open them is the ID"* – P11.

> *"If there is too much fraud or any abuse, the partner* (third party) *gets suspended. If there is a need, customers are refunded"* – P12.

> *"Where fraud is committed, the matter is also reported to SAPS* (police) *by the company or the partners* (third parties)*. If the partner* (third parties) *is involved, the contract is also canceled* – P6.

The participants mentioned that where the digital system is deficient, it is fixed via a CR process. For example, a CR was logged to stop a fraud scheme that was caused by a loophole in the customer management system. Agents were creating and cancelling sales orders multiple times, and this resulted in the credit limit of the existing customer is increased. This was done to grant credit to non-qualifying customers. It was mentioned that this was done purely to maximise sales commissions by agents.

The customers received the mobile device, while Company X was left with bad debts and potential non-compliance with the National Credit Act (NCA), Act 34 of 2005.

While the CR was being developed to fix the problem, the fraud team introduced a manual process, where each credit application was scrutinised. It was mentioned that depending on the complexity, CRs can take a few weeks to a few months to be completed. There was a consensus among participants that there must be constant fraud prevention and detection improvements because fraud schemes are constantly evolving. One of the participants indicated that there are always efforts to outsmart the fraudsters.

> *"One of the controls being considered is facial recognition, which will be matched with the* (Department of) *Home Affairs database. This will help establish ascertaining during the application process, we are dealing with the legitimate customer, and not the fraudster. The facial recognition would augment the OTP control"* – P10.

The participants mentioned that albeit prevailing challenges, there is a strong compliance process, which includes enforcement of ethical conduct through the ethics handbook. There are also data classification standards, where compliance is measured and enforced. Some aspects of digital ethics, like data privacy, data governance, and misuse of data are monitored. A participant mentioned that there are other digital ethics practices that are performed within Company X, but they are not referred to as digital ethics.

> *"There are other initiatives which fall under digital ethics, which are practiced within the Company, but we do not refer to those as digital ethics"* – P5.

It was established that some of these digital ethics initiatives are being addressed primarily by IS. The other participants were of the view that even though digital ethics practices are not perfect, nevertheless, a good foundation has been set. The pre and post implementation assessments are not exclusively focused on digital ethics, but they are nonetheless performed, albeit from a functional perspective. The participants from digital products indicated that as much digital ethics was not

formally practiced, there are processes to ensure that there is design and monitoring of digital products once they are in the market.

> *"The digital product starts as an idea, and then that idea has to be approved into a concept. From there it is formalized and then presented. Once it is approved, it is then developed. Then in development, you will follow the development stages where you will start with the design of the concept, and design of the product, and then you have your design sessions and all that, and every step gets approved. Issues of digital ethics are not discussed during the process* – P6.

> *"Once the product is launched, there are mechanisms to check risks associated with that product, like revenue generation, visibility and awareness from a marketing point of view, impact on the market, data interrogation to understand the drives behind various spikes, engagement with the partner to better understand the product"* – P12.

> *"Depending on how the product is received, six months later you do reviews, to see how it is performing based on revenue and customer feedback. If after some time, two years, or the product is not performing, then you replace it"* – P12.

The other participants indicated that the design phase was robust. There was an acknowledgement that ethical design is not fully practiced. However, some views were that there are elements of it that were practiced. They argued that when digital technologies are designed, there is an ever-present consideration of how they could be exploited for nefarious purposes. Even when digital technologies are in use, there are re-assessments conducted to improve controls. They mentioned that these are performed proactively or as a response to digital fraud that has been committed. It mentioned that double opt-in, fingerprint biometrics, OTP, and AVS were some of the controls that were conceptualised on that basis.

The participants mentioned that there are processes to receive and address customer complaints. RAFT scans the operational environment and escalates abuse or fraud to management and relevant functions. It was mentioned that other practices like Software Development Life Cycle (SDLC), quality assurance, and penetration testing is conducted by IS. One participant mentioned that even though people from diverse backgrounds do not sit in one forum, IS addresses design and other aspects as part of the SDLC processes.

> *"Information security addresses the design and other things as part of the solution lifecycle management processes" – P3.*

Most of the participants emphasised that the pre and post implementation is conducted only by IS (and digital products separately), the other functions are not involved. One participant was not convinced that the pre and post implementation was conducted by IS.

> *"There is no function or body that does quality assurance to check that the system is designed properly and is working as intended. Post or pre"* – P6.

Most of the participants indicated that IS conducts its own tests when a digital system is acquired or a digital tool is launched, using its own security checklist, without the involvement of other functions.

> *"Post implementation is not done by IT or Information Security, but not as part of digital ethics"* – P3.

> *"Information Security checks and general compatibility, including whether the acquired digital solutions will not compromise the controls of the company, but this test is not specific to digital ethics"* – P7.

Some of the participants mentioned that IS monitors and tracks 10 risk domains: which include no leakage of confidential business information, amongst others.

> *“We monitor 10 Security domains. They are data protection, security training and awareness, security operations, endpoint protection, access governance, venerability management, security testing, third-party security, perimeter and network security, and security compliance”* – P4.

There is no governance forum (DEGC) for digital ethics, and the DEF is not enforced; however, one participant indicated that the CRC does exist, but only looks at issues from a commercial standpoint. Another participant indicated that there is a PSC, which sits weekly, with the aim of managing and monitoring the digital transformation. Most of the participants emphasised that there are processes to ensure that digital technologies do not harm customers. They mentioned that the organisation is automating as many processes as possible with the aim of creating a good customer experience. The views obtained were that Company X's digital ethics practices relating to risk management, compliance with laws, audit trail, data privacy, cyber security, and so forth.

> *“We are not only prioritizing the sales generation, but that will also prioritize the things that can harm customers and the public, at the heart of that is to prioritise human rights”* – P11.

4.6.3 *Conclusion on proposition 3*

This proposition indicated that positive ethical culture, sound governance, and effective FRM practices mitigate against digital fraud, and that the organisation must use digital technologies in a manner that does not cause digital fraud. The findings are that the use of digital technologies has created certain risks and challenges which cause or might cause digital fraud. There are FRM practices that are deployed to counter the same risks and challenges. Finally, there will be substantial improvement if there is governance of digital ethics and the implementation of the DEF.

4.7 Summary of findings

Proposition 1: Organisations should practice digital ethics governance to prevent harm to stakeholders; and to protect the organisation from the consequences of failure of governance, non-compliance to laws, reputational damage, and financial loss.

The overarching finding emerging regarding this proposition is that ethical practices, whether digital or not, are not attainable without a proper governance process. The governance process is fundamental in managing, monitoring, and coordinating the different aspects of digital ethics. There is a positive organisational culture, even though there was no governance of digital ethics, and the DEF was not implemented. It is essential to eliminate the said weaknesses, to enhance the control environment and protect of harm against customers and other stakeholders.

Proposition 2: The digital ethics framework must be robust and comprehensive; it should include risk management, ethical design, responsibility allocation, founding guidelines, legal compliance, impact assessment, digital asset protection, audit trail, and post implementation monitoring.

Company X has practices relating to digital ethics, which are risk management, combined testing and reviews, access governance, and monitoring of vulnerable systems. There are also limited aspects of digital asset protection and audit trail that are practiced. There are positives and negatives in how the organisation practices some of the mentioned aspects of digital ethics. It was found that the digital ethics practices are not formal, uniformed, or structed, and this was attributed to the absence of digital ethics governance, non-implementation of the DEF, and that the digital strategy is not anchored by the DEF.

Proposition 3: The positive ethical culture, sound governance, and effective FRM practices are primary mitigators of digital fraud; the organisation must not use digital technologies in a manner that causes the risk of digital fraud.

Based on the views of the participants, the risks and causes of digital fraud are mitigated as reflected in Table 13. The views of the participants indicate that Company X's use of digital technologies has created certain risks and challenges which cause or might cause digital fraud. The table details the risk, causes, and mitigation that has

been deployed by the incumbent organisation to ensure that it does not use digital technologies in a manner that causes digital fraud.

Table 13: Risks, causes, and mitigating controls

Risks	Causes	Key Mitigation Controls
1. Lack of proper access to governance	• Unauthorised access to both the network and systems, because of poor password management, which includes the ease with which a password can be changed. This includes the sharing of logging credentials between agents and employees. • Non-removal of user profiles of resigned employees, non-amendment of user profiles of employees who have moved to other departments	1. Penetration testing 2. Regular access reviews 3. AD, MFA, and access control for different applications, 4. VPN as an added layer to access the organisational network. 5. Endpoint security, perimeter and network security, vulnerability system management, third-party security and data protection. 6. Managers have a responsibility of monthly checking the access that their direct reports have. 7. Same network log-in and the system log-in to control to counter the sharing of logging credentials.
2. Abuse of system and processes	• Lack of segregation of duties and abuse of systems to create unauthorised transactions by employees and third-party employees.	1. IT policy, which regulates what should be done and not done. 2. Monitoring of systems that are susceptible to abuse. 3. The customer system is being monitored for abuse by RAFT and others. 4. Monitoring transactions performed on the customer management system. 5. Issuing and canceling orders report, which includes checking compliance with the credit vetting policy. 6. Same network log-in and the system log-in to control to counter the sharing of logging credentials.
3. Data privacy or data governance	• Improper disposal of information or leak of confidential information with outside parties.	1. Enforcement of ethical conduct via the ethics handbook. 2. Data classification standards, 3. Limited aspects of digital ethics, like data privacy, data governance, and misuse of data 4. Application security standards require tools and systems to have an audit trail.
4. Subscription and general digital fraud	• Employees and agents colluding with external fraudsters. • Identity fraud • Banking fraud	1. Double opt in control - protection for unauthorised charges to customers. 2. Fingerprint biometrics, AVS, debi-check and OTP 3. Delinquent third party: loss recovery, criminal case, and disciplinary hearing 4. Non-payment on the first debit order, the fraud team ascertained that the failure was not due to fraud. 5. Block system access for delinquent third-party users

		6. Targeted communication and awareness of fraud trends to various stakeholders 7. Invoices are digitized and encrypted. 8. Continuous system improvements through CRs 9. Exception reports every two hours by RAFT. 10. Sim-swaps only performed at the stores
5. Inefficient and ineffective digital practices	• Employees' resistance to change due to change management. • Lack of ethical design • No consideration for algorithm bias • No involvement of diverse functions • Insufficient training and awareness • Lack of pre and post implementation assessment. • Incident communication • Digital Opportunities vs digital harm	1. Creating awareness about digital scams 2. There are mechanisms to check the performance of digital products once they are launched. 3. The pre and post implementation are separately conducted by digital product and IS. 4. Proper design of products (but not from the digital ethics perspective). 5. Limited elements of ethical design are practiced, like customer consent, data privacy, and data governance. 6. There is ever-present consideration of how digital technologies could be exploited or abused. 7. SDLC, quality assurance, and penetration testing are conducted. 8. IS checks systems compatibility, and whether acquired solution will not compromise the control environment. 9. IS conducts tests using its security checklist when a system is acquired. 10. Ten Security domains are monitored. 11. Monitoring of critical or showstopper applications by IS 12. Consequence management against those that are implicated. 13. CRC and PSC do exist but primarily look at issues only from a commercial perspective. 14. There is a limited process to ensure that digital technologies do not harm customers.

CHAPTER 5. DISCUSSION OF THE FINDINGS

5.1 Introduction

This chapter discusses and explains the findings of the study that was analysed in the preceding chapter. The discussions and explanations are presented as per the three propositions and the themes of the study. A common thread was maintained between the research questions, proposition, and themes as reflected in Table 14.

Table 14: The research questions, propositions, and themes

Research questions	Propositions	Themes
Research question 1 How is governance of digital ethics practiced in Company X?	**Proposition 1:** Organisations should practice digital ethics governance to prevent harm to stakeholders; and to protect the organisation from the consequences of failure of governance, non-compliance to laws, reputational damage, and financial loss.	1. Governance 2. Non implementation of DEF 3. Organisational Culture 4. Incidence Reporting
Research question 2 What are the components of the digital ethics framework in Company X?	**Proposition 2:** The digital ethics framework must be robust and comprehensive; it should include risk management, ethical design, responsibility allocation, founding guidelines, legal compliance, impact assessment, digital asset protection, audit trail, and post implementation monitoring.	5. Risk Management 6. Combined Reviews & Testing 7. Access governance and priority systems management
Research question 3 How are the risks and causes of digital fraud mitigated in Company X?	**Proposition 3:** A positive ethical culture, sound governance, and effective FRM practices are primary mitigators of digital fraud; the organisation must not use digital technologies in a manner that causes the risk of digital fraud.	8. Digital ethics risks and challenges 9. Digital ethics practices

5.2 Discussion pertaining to Proposition 1

Proposition 1 indicates that: **Organisations should practice digital ethics governance to prevent harm to stakeholders; and to protect the organisation from the consequences of failure of governance, non-compliance to laws, reputational damage, and financial loss.**

5.2.1 *Governance*

The study ascertained that there is no governance of digital ethics, other than the existence of the DEF, which was not implemented, and therefore not in force. Despite the absence of the governance of digital ethics, there is proper governance of conventional corporate ethics, ERM, IT, IS, and other functions. There is an Ethics Officer, who is responsible for corporate ethics, but not digital ethics. There is no DEGC, but there is ITEB, ISC, and GRC, which are concerned with IT, IS, and ERM, but without a specific focus on digital ethics. There was a universal acknowledgement from participants, which is corroborated by the literature that digital and corporate ethics, should be managed from the same place (Eitel-Porter, 2021). It was established that there are current processes in place to amend the terms of reference of ISC and/or other relevant forums to cater to digital ethics.

The responsibility of digital ethics must be isolated to the DEO, who must also chair the DEGC (Stahl, 2022). The DEO is also the custodian of the DEF (Stahl, 2022). The literature further indicates that there is no difference between the governance of digital ethics and that of conventional corporate ethics, however, organisations should strive to make a distinction between the two (Schiff et al., 2020). Eitel-Porter (2021) argued for the use of existing ethics governance structures, rather than creating separate digital ethics structures, as this would create duplications. In Company X, there is a distinction between digital ethics and corporate ethics; there are governance forums for the latter, but, nothing for the former.

The study established that the governance processes are focussed on IS and IT, and not digital ethics. The works of the governance forums (ITEB, ISC, GRC) feed into the quarterly report of the RC. There is also the CRC and PSC, but their focus is mostly commercial. The DEF was approved by the SEC in February 2023, but there is no

reporting to the SEC relating to digital ethics. SEC receives quarterly reports on corporate ethics.

SEC is the equivalent of the Ethics Board as advanced by Eitel-Porter (2021), which must also be responsible for digital ethics. In terms of King IV, corporate ethics is the responsibility of the SEC. The DEGC should report to the SEC. As indicated there is no DEGC in the incumbent organisation. None of the mentioned existing governance forums are the equivalent of the DEGC, this is because they are not explicitly focussing on digital ethics. In addition to that, none of these governance forums include people from diverse functions like technologists, legal, ethics, and business experts as suggested by Blackman and Ammanath (2022).

5.2.2 *Non implementation of DEF*

The key finding is that the DEF exists but was not implemented, yet it was found that it was developed to ensure that digital products and services are managed and offered in an ethical manner. The non implementation of the DEF was ascribed to resistance from BUs, lack of funds, fear of digital technologies, and lack of change management. The other cause was attributed to digital ethics being a new concept, and that not many people know about it. This was worsened by the fact that the existence of the DEF was not sufficiently communicated, and as a consequence of that, not many people know about its existence. It was said that the DEF will be implemented at a later stage.

Company X DEF has the following 10 guidelines: autonomy, justice, beneficence, non-maleficence, and transparent, and that it is further guided by the following principles competence; responsibility; accountability; fairness; and transparency. Of the 10, two of them, beneficence and competence do not appear in the five guidelines identified by Jobin et al. (2019), the 14 identified by Ashok et al. (2022), and the 10 identified by Armstrong and Lee (2022) as reflected in Table 2.

Of the remaining eight, three were in the consolidated guidelines of Jobin et al. (2019), Ashok et al. (2022), and Armstrong and Lee (2022), as indicated in Table 3. The remaining five were in the individual guidelines of the said researchers as follows:

Accountability was mentioned in the Ashok et al. (2022) guideline; non-maleficence, fairness, responsibility, and justice were mentioned in the Jobin et al. (2019); fairness and transparency was mentioned in the Armstrong and Lee (2022) guidelines. Those that are in the consolidated digital ethics guidelines, and not part of the Company X DEF is, no physical harm or compromise of safety, privacy, regulatory impact, individual and societal impact, and financial and economic impact. Bar the said guidelines that were omitted, Company X DEF has most of the fundamental guidelines that are advocated by the cited literature.

5.2.3 *Organisational Culture*

The organisational culture describes how the organisation does things (Bamidele, 2022). Armstrong and Lee (2022) posit that organisational culture is the primary pillar for any organisation that wants to succeed in the digital world. It was found that there are practices that have a positive contribution to the organisational culture, and equally there are those that have a negative contribution. However, overall, most of the participants mentioned that the incumbent organisation has a positive organisation culture. This is important because the research shows that organisational governance enables positive ethical culture (IoDSA, 2016).

The organisation has an ESG program, and an ethics handbook, which has corporate governance sections relating to the declaration of gifts, conflict of interests, fraud, and corruption, and whistleblowing. The study found that where progress is lacking in the implementation of recommendations of assurance providers, ERM engages management to ensure that they are implemented. There is a positive leadership tone and consequence management against implicated parties. The significance of these on organisational culture is supported by literature, which found that the amount of fraud perpetrated in an organisation is dependent on the ethical culture; the higher the ethical culture, the lesser the incidents of fraud (Ndlovu, 2020; Cavaliere et al., 2021). In the same vein, according to Bezuidenhoud and Geldenhuys (2019) and Fourie (2019), the creation of a positive ethical climate is dependent on the correct leadership tone among other things, which is the case in the incumbent organisation.

The study established that the negative contributions to the organisational culture that needed improvement were that the organisation is conservative, and employees are

generally resistant to change. It was ascertained that ethics and fraud awareness and training were not impactful, because they are predominantly conducted via corporate communications emails. Lastly, it was found that there was no sufficient oversight of the work performed by the third parties. All these need to be addressed because the literature indicates that negative factors weaken governance and internal controls, and creates a fertile ground for conduct that is inconsistent with the values of the organisation (Marzuki et al., 2020).

5.3 Results pertaining to Proposition 2

Proposition 2 indicates that: **The digital ethics framework must be robust and comprehensive; it should include risk management, ethical design, responsibility allocation, founding guidelines, legal compliance, impact assessment, digital asset protection, audit trail, and post implementation monitoring**.

5.3.1 *Risk Management*

The study found that there is no specific digital ethics risk register, however, there are risk registers for IT, IS, and other risks facing the organisation. Risk management is governed by the ERM forum, GRC, and RC. The views of participants were that where there was digital harm, management intervened and addressed the problem. There is a digital strategy, and the PSC is responsible for maximising digitisation opportunities and minimising the corresponding risks. It was established that the assessments or tests of digital harms are erratic, and narrow, and they are mostly performed by IT and IS. The said practice is not accordant with Winfield et al. (2019) and Eitel-Porter (2021) who submits that digital technologies must be tested by a diverse team to ensure that all risks are taken care of.

The absence of dedicated risk management of digital ethics creates a risk that Company X might not fully mitigate the consequences of the use of digital technologies. The risk management processes are not embedded from the initiation until post implementation of digital technologies. The negative consequences of the use of digital technologies can be dealt with if there is a proactive application of digital ethics (Floridi,

2018). The non-implementation of DEF, including the absence of a digital ethics risk register, suggests that the organisation does not maintain a balance between the positives and negatives of digital transformation as suggested by Becker et al. (2022).

They were contrasting findings as to whether the incumbent organisation sufficiently communicates incidences of digital fraud, as part of the broader management of FRM. The views obtained were that there must be improvement in that regard, specifically communication to customers and members of the public. The literature indicates that transparency by the organisation enables trust, legitimacy, and a good reputation (Alsayegh et al., 2020). Therefore, as required by the stakeholder theory, the sharing of information in this regard is in the interest of the incumbent organisation. Based on that, Company X should consistently communicate to customers and members of the public warnings and digital fraud trends prevailing in the industry at that specific time (Yonder, 2023).

It was found that the organisation has detailed ethics and fraud training and awareness initiatives, however, some participants argued that this was not enough, specifically cyber security awareness to employees and third parties. Buil-Gil et al. (2021) indicated that organisation that prioritises ethics and fraud awareness and training, experiences fewer incidences of digital fraud. The heightened awareness of stakeholders, and other FRM measures, are pivotal in eradicating digital fraud (Graydon, 2020). In the case of the incumbent organisation, these initiatives must be extended to all and sundry including third parties.

5.3.2 *Combined Reviews and Testing*

The results obtained from the testing of digital technologies must be used to mitigate digital ethics risks (Winfield et al., 2019). The findings in this regard are consistent with the literature. It was found that there is limited pre and post implementation testing of digital technologies. Even when they are tested, the testing is only conducted separately by IT, IS, or the digital products team, without the involvement of other functions. The functions like ethics, fraud, and others are not involved. The non-involvement of other functions shows itself in how the PSC and other committees are composited. The other view obtained was that other functions are invited to the said committees when there is a need.

The literature indicates that the combined reviews and testing are at the centre of the governance of digital ethics and must be executed within the auspices of the DEGC. The combined reviews and testing processes must be transparent, and holistic, and must they consider the positives and negatives of digital technologies (Winfield et al., 2019; Eitel-Porter, 2021). The absence of properly combined reviews and testing s might cause misuse, poor design, poor development (Winfield et al., 2019; Eitel-Porter, 2021); algorithm bias, and lack of audit trail (Schiff et al., 2020). There was an acknowledgement from most participants that properly combined reviews and testing must be consistently and comprehensively conducted to improve the practices of digital ethics.

5.3.3 *Access governance and priority systems management*

The robust authentication process is a prerequisite for ensuring that proper access is granted to people that require access to the digital systems of the organisation (Detura et al., 2022). The prevention of digital fraud and general misconduct starts with regulating both physical and logical access. Most respondents indicated that the incumbent organisation has a challenge of sharing log-in credentials; non-removal of user credentials of people that have left the employ of the organisation; and non-updating of user profiles for employees that have changed roles or moved to other departments. Furthermore, it was established that the process of changing passwords is weak. It was also established that these challenges contribute to irregular conduct and the commission of digital fraud within Company X.

The said challenges are ensuing despite the organisation having AD, MFA, VPN, and regular access reviews, amongst others. On a monthly basis, managers also check whether their direct reports have the correct access profiles. It was found that the said controls are largely compromised by human conduct. Despite these setbacks, the organisation must continue making investments and improvements in its digital ethics and FRM practices. The said investment will help protect the organisation from various types of fraud risks (Buil-Gil et al., 2021), especially because Company X is in the midst of executing its digital strategy. The more the organisation digitises and increases its

digital touchpoints, the higher the chances of being victims of digital fraud (Buil-Gil et al., 2021).

RAFT monitors that vulnerable systems are not abused, by reviewing and actioning exception reports based on the anomalies identified. Once there is evidence confirming the anomalies identified, they are sent to management or the forensics unit. Where there is substantive evidence of wrongdoing, consequence management measures are meted against the implicated parties. These fraud detection measures deployed by Company X are supported by the literature. Batra et al. (2020) postulate that secure systems and networks can be improved with the application of ML and data analytics. In addition to that, the literature indicates that organisations that invest in building internal capabilities, respond much better to cybercrime than organisations that do not (Buil-Gil et al., 2021).

5.4 Results pertaining to Proposition 3

Proposition 3 indicates that **A positive ethical culture, sound governance, and effective FRM practices are primary mitigators of digital fraud; the organisation must not use digital technologies in a manner that causes the risk of digital fraud.**

5.4.1 *Digital ethics risks and challenges*

The findings obtained from the study revealed that the primary digital ethics risks and challenges faced by organisation were the following: no governance of digital ethics; DEF was not implemented; and digital ethics training was not conducted. The absence of digital governance created a lack of transparency on whether there was a balancing act of considering both the positives and negatives of digital technologies (Winfield et al., 2019). As a result of this, it was established that digital ethics practices were not intentional, mature, structured, and uniformed. As mentioned by the literature, this was because there was no true north in the form of DEF to ensure that digital ethics practices withstand varying circumstances (Becker et al., 2022).

It was ascertained that the ripple effect of the main digital ethics risks and challenges faced by the organisation was the manifestation of the following secondary digital ethics risks and challenges: access governance challenges; lack of segregation of

duties; lack of distraction or disposal of the information; various employees' misconduct, including sharing of logging credentials; poor management of third parties; resistance to change; insufficient, or non-existence monitoring of data privacy and misuse algorithm bias.

The literature indicates that fraud and crime in general is an ever-present reality in society. No one is immune to it, especially digital fraud which affects millions of people because of its pervasive nature (Kemp, 2020; Cavaliere et al., 2021; Batra et al., 2020). There primary and secondary digital ethics risks and challenges mentioned had an impact on digital fraud. The participants indicated that subscription fraud manifested itself in multiple ways, including identity and application fraud, as ascertained by Thompson (2022) and Libera (2020). The digital fraud that is experienced by the incumbent organisation is consistent with the SAFPS (2023) report, which found that digital fraud was on the rise. SAFPS (2023) found that identity fraud has increased by 300% between 2021 and 2022. The organisation also experiences other types of fraud, which include phishing, sim-swap fraud, porting fraud, account take-over, profile building, and others as highlighted by Graydon (2020), Batra et al. (2020), and Khadas (2020).

Digital fraud is perpetrated from multiple fronts. The study found that digital fraud is perpetrated by employees, third parties and their employees, and customers and members of the public. This is also confirmed by the findings of Ahmad (2020) and Mabuza (2021), who ascertained that digital fraud schemes are orchestrated by internal and external actors. Furthermore, the PWC (2022) report established that 43% of digital fraud is perpetrated by external fraudsters, 31% by internal fraudsters, and 26% by collusion between internal and external fraudsters.

The study found that there are various initiatives within the organisation to lessen the impact and damage of fraud on business operations. The findings indicate that digital fraud has a devastating impact on the following: reputational damage, negative customer experience, financial loss, ethical culture, non-compliance to POPIA, and so forth. These findings are the same as those advanced by Abubakari (2021), Detura et al. (2022), Graydon (2020), Mostafa (2022)

5.4.2 *Digital ethics practices*

Graydon (2020) argued that organisations cannot look for answers elsewhere concerning fraud prevention other than from itself. The practices of the organisation are aligned with that of the said researcher, as reflected in Table 13. The study found digital ethics practices that are aimed at preventing harm to stakeholders, albeit not intentional, mature, structured, and uniformed. Some of the positive digital ethics practices highlighted by participants are the following: IT acceptable use policy; performance of vulnerability checks and penetration testing; exception reports to monitor systems that are susceptible to abuse; enforcement of ethical conduct through the ethics handbook; data classification standards; data privacy, data governance, misuse of data is monitored as part compliance to POPIA; and monitoring of 10 cyber security domains.

There are also digital ethics practices within the incumbent organisation that are not practiced in alignment with literature, specifically specific elements of digital ethics reflected in Figure 2. Those elements were put forward by Armstrong and Lee (2022), Winfield et al. (2019), Eitel-Porter (2021), Mišić (2021), IEEE (2017), Stahl (2022), Floridi (2018), Stahl (2022), Li (2023), and Ashok et al. (2022). Those that do not fully satisfy the literature relate to limited alignment between digital and corporate ethics; limited, functional, and non-diverse based pre and post implementation assessments; limited design process; and limited communication to stakeholders.

The findings reveal that Company X has copious initiatives that are geared at fraud prevention, fraud detection, and investigation. These controls include authentication of users; training and awareness; employee and third-party code of conduct; whistleblowing and investigation of allegations; exception reporting; various types of policies, including the credit vetting policy; various types of application and bank account verification controls; and system reviews and improvements via CRs.

According to most participants, the organisation has zero tolerance towards unethical conduct and fraud. Consequence management is dispensed to delinquent stakeholders. The said consequences include disciplinary proceedings, recovery of losses, civil proceedings, criminal action, and removal of system access specifically for third-party employees. These measures must be enhanced to prevent, detect, and

deter digital fraud. This is because there is a general lack of consequences for those who commit digital fraud in society (Babanina et al., 2021), and this breeds impunity. The strengthening of these measures will ensure that the organisation remains faithful to its zero-tolerance stance towards fraud and irregular conduct. Furthermore, it will help direct the digital fraud traffic from the incumbent organisation to organisations that do not have these measures.

5.5 Conclusion

The appropriate practices of digital ethics are essential to mitigate the harm that might be caused by digital fraud. There are good digital ethics practices within the incumbent organisation, but they are negated by the absence of governance of digital ethics, non-implementation of the DEF, and the lack of training and/or knowledge about digital ethics. It is crucial that the execution of the digital strategy of the organisation is supported by the good digital ethics practices advocated by the literature. There is no better protection that can be accorded to stakeholders relating to harms of digital fraud, than the improvement of practices concerning risk management, combined testing and reviews, access governance, and the monitoring of priority or vulnerable systems.

CHAPTER 6. CONCLUSIONS & RECOMMENDATIONS

6.1 Introduction

This is the last chapter of the study that details conclusions based on the research questions, literature review (Chapter 2), presentation of findings (Chapter 4), and the discussion of findings (Chapter 5). It also details the recommendations and suggestions for future research. Based on the problem statement and research questions outlined in Chapter 1, the discussion addresses the application of digital ethics practices to mitigate digital fraud in an MNO in South Africa.

The research problem was that the lack of adoption of digital ethics practices leads to possible digital fraud because the risks of digital technologies are not mitigated. To prevent that from happening, the literature indicated that the organisation must embrace the stakeholder theory because it avoids harm by considering the interest of stakeholders (Valentinov, 2022). The organisation can adopt digital ethics practices that will mitigate digital fraud if there is a positive ethical culture that permits effective corporate governance (Ndlovu, 2020), supported by the correct leadership tone and values (Bezuidenhout and Geldenhuys, 2019; Fourie, 2019).

The stakeholder theory does not seek market success at all costs. It was cited that the stakeholder theory allows and from communication between the organisation and stakeholders. This then fosters learning and the cultivation of good relationships between the parties (Freeman et al., 2021). The transparency, communication, and good relationship between stakeholders facilitate the establishment of trust, legitimacy, and good reputation (Alsayegh et al., 2020). The benefits accorded by the stakeholder theory, plus the positive organisational ethical culture and corporate governance generate a favourable environment for the effective governance and practice of digital ethics and FRM.

6.2 Conclusions regarding research question 1

The research question: how is governance of digital ethics practiced in Company X?

There is an absence of governance of digital ethics in Company X. The literature emphasised the importance of governance as a pre-requisite for success. There is proper governance of corporate ethics, IS, IT, and others, but nothing for digital ethics. The practices of the incumbent organisation are antithetical to the literature because there is no uniformity in the way digital and corporate ethics are governed. The management level governance forums and SEC receive reports relating to corporate ethics, but nothing related to digital ethics. Due to that fact, there are matured processes on the management and oversight accorded to corporate ethics. However, the absence of governance of digital ethics creates a significant dent in the overall management of ethics in the organisation.

The digital ethics responsibility is not isolated to a senior person, who is the equivalent of the DEO, as required by the literature. However, there is a senior person in the form of an Ethics Officer, who is the custodian of corporate ethics. As mentioned by the literature, and advocated by participants, there must be no difference between the governance of digital and corporate ethics. The absence of digital ethics governance is compromising the digital strategy, which should be insulated from various ills by the effective practices of digital ethics.

The DEF is not yielding any benefits and is as good as not existing. The study found that employees were not aware of its existence, including those who are involved with digital technologies, products, risk, ethics, IT, and IS. It was cited that the DEF is a guiding instrument, that is supposed to guide the organisation in its digital transformation. In its absence, there is a risk that digital technologies might be used in an unethical manner, or the organisation might not have adequate processes to prevent and detect digital fraud. The implication of this is that stakeholders might be harmed. The study revealed that even though the DEF of Company X was not implemented, it nevertheless has most of the fundamental guidelines that are advocated by the literature. In that case, the implementation of the DEF will

substantially enhance the practices and governance of digital ethics in the organisation.

In addition to corporate governance, the literature recognises organisational culture as the foremost requirement for market success. As much as it was found that overall, the organisation has a positive ethical culture, however, this is negated by the non-governance of digital ethics and non-implementation of DEF. The literature noted that there is a positive correlation between the organisational culture and the extent of fraud in the organisation. It is for that reason that the said weaknesses must be improved to bolster organisational culture.

6.3 Conclusions regarding research question 2

The research question: What are the components of the digital ethics framework in Company X?

The study established that Company X has 10 guidelines, which are autonomy, justice, beneficence, non-maleficence, transparency, competence; responsibility; accountability; fairness; and transparency. Due to the fact that DEF was not implemented, the said guidelines are not applied. The study found that the organisation practices limited elements of the following components of digital ethics: risk management, combined testing and reviews, access governance, and monitoring of vulnerable digital systems. There was also evidence of digital ethics practices relating to digital asset protection and audit trails. It was established that some components of digital ethics require substantial improvements because the practices thereof are not aligned with the literature. Those components are ethical design, responsibility allocation, and impact assessments.

It was cited that the components of DEF must be robust and comprehensive. This is not the case in the organisation, because it was established that not all the mentioned components are practiced, or they were practiced in a manner that is not aligned with the literature. The shortcomings thereof might expose the organisation to digital fraud, financial loss, and non-compliance to POPIA, amongst others. The combined reviews and testing were identified by the literature as the core of the governance of digital ethics. It was further cited that testing must be transparent, and holistic, and must

consider the positives and negatives of digital technologies. Contrary to the literature, there is limited pre and post testing or assessment of digital technologies. It was found that the assessments of digital harms were erratic, non-comprehensive, and executed from a narrow functional perspective.

The study revealed areas where the organisation is on the right track and areas where minimal improvements are warranted. It was apparent that there are sound risk management processes, despite the absence of the specific digital ethics risk register. It was found that where there was digital harm, management intervened and addressed the problem. This was consistent with the finding that there is a positive leadership tone from management, illustrated by the existence of numerous consequence management initiatives. As supported by the literature, there are fraud detection data analytics mechanisms executed to monitor that vulnerable systems are not exploited to the detriment of the organisation. The literature indicated that organisations that have internal capabilities respond better to digital fraud compared to those that do not. However, the non-existence of a digital ethics risk register detracts from the said sound risk management processes. The absence of a digital ethics specific register implies that there is no balance between the positives and negatives of digital transformation as required by the literature.

The study found that the organisation was inconsistent in communicating with its stakeholders about the incidences of digital fraud, specifically external stakeholders. This is not aligned with the dictates of the stakeholder theory. The were weaknesses found relating to fraud training and awareness, specifically relating to cyber security awareness to employees and third parties. This requires an improvement because it was cited that organisations with heightened ethics and fraud awareness and training experience less fraud incidence.

The literature mentioned the importance of ensuring that access is granted to the correct persons. The incumbent organisation has invested in controls like AD, MFA, VPN, regular access reviews, and others. Despite that, some respondents noted that there are challenges relating to access governance in the organisation. The study revealed that this was a key contributor to irregular conduct and the commission of

digital fraud within Company X. The participants revealed that in the main, the said internal controls are largely undermined by human conduct. This necessitates the importance of strengthening cyber related awareness training as suggested by some participants. The awareness training will help address the findings of lack of knowledge of digital ethics and lack of change management. The investment in this regard must be perpetual as cited by the literature because a heightened level of awareness will insulate the organisation from fraud risks. This is a non-negotiable imperative because organisations must galvanise their internal stakeholders to increase the chances of success of the digital strategy.

6.4 Conclusions regarding research question 3

The research question: How are the risks and causes of digital fraud mitigated in Company X?

The use of digital technologies inadvertently attracts certain risks, one of which is fraud risk. The findings indicate that the primary risks and challenges of Company X are a lack of governance of digital ethics; non implementation of DEF; and the lack of digital ethics specific training. It was also found that the organisation's secondary digital ethics risks and challenges are access governance challenges; lack of segregation of duties; lack of distraction or disposal of information; sharing of logging credentials; poor management of third parties; resistance to change; insufficient monitoring of data privacy breaches and algorithm bias. As indicated above, there are digital ethics practices that are deficient and not aligned with the literature. A full list of those includes limited alignment between digital and corporate ethics; limited, functional, and non-diverse pre and post implementation assessments; limited design process; and limited communication to stakeholders. These deficient digital ethics practices contributed to the existence of the mentioned risks and challenges.

These risks and challenges have caused digital ethics practices not to be intentional, mature, structured, and uniformed. It was cited that the DEF guides and directs the organisation to be faithful to the committed course, in its absence the organisation will not be able to withstand varying digital ethics risks and challenges. The literature indicated that digital fraud is a pervasive force that is perpetrated by internal and

external actors in the organisation, which manifests via multiple illicit schemes to the detriment of millions of people. Digital fraud increases the cost of conducting business; furthermore, the literature indicates that it impugns the ethical culture, reputation, and customer experience, and causes financial loss, and non-compliance with laws. Based on the said consequences, organisations have no choice but to craft fraud prevention and detection measures to restrain digital fraud.

There are multitudes of internal controls that are employed by Company X to mitigate digital fraud. Most importantly, it was found that the organisation has committed itself to zero tolerance towards unethical conduct and fraud. There are consequences against implicated parties, and these include disciplinary proceedings, recovery of losses, civil proceedings, criminal action, and other measures. This practice is aligned with the literature. The controls geared at countering the risks and challenges range from IT acceptable use policy; vulnerability checks and penetration testing; system abuse and manipulation exception reports, ethics specific policies; data governance, POPIA compliance, and monitoring of 10 cyber security domains.

Despite concerns raised by participants on shortcomings relating to the authentication of users and training and awareness as indicated above, nevertheless there are controls and activities relating to those. The other controls mentioned by participants were employee and third-party codes of conduct; whistleblowing and investigation of allegations; several types of policies, and system reviews and improvements via CRs. The literature noted that digital fraud is increasing. On account of that, internal controls must be constantly reviewed and enhanced. The main concern is that the mentioned controls and other measures deployed by Company X are stunted by the primary and secondary digital ethics risks and challenges. Those needs to be mitigated to ensure the efficiency and effectiveness of the said controls.

6.5 Recommendations

1. Enhancement of the organisation culture

A positive organisational culture is a germane because as established from the literature, it augments the chances of market success, and it causes the organisation to experience fewer incidences of fraud. Accordingly, in addition to the digital ethics framework and governance, Company X must implement, monitor and improve activities that enhance the organisational culture. From the study, it was apparent the organisation commits to zero tolerance towards fraud and unethical conduct, a positive leadership tone, and a myriad of consequence management initiatives. However, that needs to be reflected in all layers of management, and the consequences against those implicated must be consistent and transparent as indicated by one of the participants. There is a compelling need to also improve change management processes, the understanding of digital ethics, and the wider cyber awareness and training among employees and third parties. The organisation needs to find appropriate and measurable mechanisms to communicate the incidence of fraud that have an impact on customers and members of the public. That level of transparency is consistent with the demands of the stakeholder theory.

2. Implementation of digital ethics governance

There is a pressing obligation for the organisation to formalise the governance of digital ethics. This obligation stems from the requirements of King IV relating to the governance of ethics. From the study, it is apparent that Company X has matured its corporate ethics processes. In line with the requirements of the literature and views expressed by the participants, both corporate and digital ethics must be managed and governed in the same place. Although there is a requirement for a distinction between the two, there is no need for separate committees and governance processes, as that might cause duplications and confuse employees. The implementation of digital ethics governance must also address issues relating to the composition of the DEGC, the appointment of the DEO, and the reporting to the SEC. In the case of Company X, the Ethics Officer, if need be, can also serve as the DEO.

3. Implementation of digital ethics framework

The good news is that the incumbent organisation does not have to develop the DEF from scratch, it just must implement the existing one, and improve where required in relation to the components of the framework reflected in Figure 2. The DEF would fundamentally prevent the unethical use of digital technologies for the benefit of the organisation and the stakeholders. The DEF would aid the organisation as it executes its digital strategy and its broader digital transformation initiatives, including the ESG commitments. Therefore, the organisation must sustain the digital ethics practices it was performing correctly in line with the literature, improve those it was not performing correctly, and start introducing those it was not performing. If all these are addressed, the organisation would have tackled the research problem head-on, by ensuring that there is an adoption of digital ethics practices that mitigates the irresponsible use of digital technologies to prevent the harm of digital fraud to the organisation and stakeholders. This would also align the organisation to the dictates of the stakeholder theory.

4. Enhancement of risk and FRM processes

The literature indicated that organisation that have internal capabilities experience less fraud than organisations that do not. From the study, it was apparent that Company X has considerable internal capabilities albeit negated by the lack of digital ethics framework and governance. The organisation should implement further measures to augment the current risk and FRM internal capabilities, and this would contribute to addressing the primary and secondary digital ethics risks and challenges. Therefore, management should consider implementing the following: a digital ethics risk register, measures that mitigate against the causes of user authentication breaches, appointment of a diverse multi-functional team that would address ethical design, and pre and post implementation testing. These initiatives are central in ensuring that there is a consideration of the positives and negatives of digital technologies that would arrest the incidences of digital fraud.

6.6 Suggestions for further research

Based on the study, the following are areas that have been identified for further research:

1. A study on the practices of digital ethics to mitigate other types of operational risks other than digital fraud or fraud risk.
2. A study that will compare financial performance and the number and extent of digital fraud between two organisations, that are in the same industry. The one organisation should have a digital ethics framework and governance and the other one should not.
3. A study on the guidelines that should be adopted by the SEC or the Board in measuring the implementation and effectiveness of digital ethics in the organisation.
4. A study of the impact of digital ethics in South Africa, and whether the South African government should promulgate legislation relating to digital or AI ethics or embrace self-regulation as adopted by other jurisdictions.

REFERENCES

Abubakari, Y. (2021). The reasons, impacts and limitations of cybercrime policies in Anglophone West Africa: a review. *Social Space Journal.EU*

Ahmad, A. H., Masri, R., Zeh, C. M., Mohd, Shamsudin, F., & Fauzi, R. U. A. (2020). The Impact of Digitalization on Occupational Fraud Opportunity in Telecommunication Industry: A Strategic Review. Palarch's Journal Of Archaeology Of Egypt/Egyptology, 17(9).

Alsayegh, M. F., Rahman, R. A., & Homayoun, S. (2020). Corporate Economic, Environmental, and Social Sustainability Performance Transformation through ESG Disclosure. *Sustainability*, *12*. https://doi.org/doi:10.3390/su12093910

Anneroth, M. (2022). *HOME ERICSSON BLOG ETHICAL AI FRAMEWORKS: A CRITICAL DIMENSION FOR DESIGNING AI FOR TELECOM*. Ericsson. Retrieved 04 June 2023 from https://www.ericsson.com/en/blog/2022/4/ethical-frameworks-ai-telecom

Armstrong, B., & Lee, G. J. (2022). *Digital Transformation And Maturity* (1st Edition ed.). Silk Route Press. Johannesburg

Ashok, M., Madan, R., Joha, A., & Sivarajah, U. (2022). Ethical framework for Artificial Intelligence and Digital technologies. International Journal of Information Management, 62 (2022) 102433.

Aspers, P., & Corte, U. (2019). What is Qualitative in Qualitative Research. Qualitative Sociology.

Babaei, K., Chen, Z., & Chen, Z. (2020). A Study of Fraud Types, Challenges and Detection Approaches in Telecommunication. Journal of Information Systems and Telecommunication, 7(4), 248-261.

Babanina, V., Tkachenko, I., Matiushenko, O., & Krutevych, M. (2021). Cybercrime: History of formation, current state and ways of counteraction. *Amazonia Investiga*, *10*(38). https://doi.org/https://doi.org/10.34069/AI/2021.38.02.10

Bamidele, R. (2022). *Organisational Culture*. Fab Educational Books. Awka, Anambra State Nigeria

Batra, S., Gupta, M., Singh, J., Srivastava, D., & Aggarwal, I. (2020). *An Empirical Study of Cybercrime and Its Preventions* Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC)

Baxter, P., & Jack, S. (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. The Qualitative Report, 13(4), 544-559.

Becker, S. J., Nemat, A. T., Lucas, S., Heinitz, R. M., Klevesath, M., & Charton, J. E. (2022). A Code of Digital Ethics: laying the foundation for digital ethics in a science and technology company. *AI & SOCIETY*. https://doi.org/10.1007/s00146-021-01376-w

Bezuidenhoud, L., & Geldenhuys, D. (2019). Identifying Organisational Climate Elements that can be used to Detect and Prevent Management Fraud. *South African Business Review*, *23*, 28. https://doi.org/https://doi.org/10.25159/1998-8125/4269

Blackman, R., & Ammanath, B. (2022). Ethics and AI: 3 Conversations Companies Need to Have. *Business Ethics*. https://hbr.org/2022/03/ethics-and-ai-3-conversations-companies-need-to-be-having

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, *9*(2), 27-40. https://doi.org/10.3316/QRJ0902027

Braun, V., & Clarke, V. (2012). Thematic Analysis. *APA handbook of research methods in psychology*, *2*, 57-71.

Buil-Gil, D., Lord, N., & Barrett, E. (2021). The Dynamics of Business, Cybersecurity and Cyber-Victimization: Foregrounding the Internal Guardian in Prevention. *An International Journal of Evidence-based Research, Policy, and Practice*, *16*(3), 286-315. https://doi.org/10.1080/15564886.2020.1814468

Cameron, D. R. (2011, 7-9 December 2011). *AN ANALYSIS OF QUALITY CRITERIA FOR QUALITATIVE RESEARCH* ANZAM - Australian and New Zealand Academy of Management - 25th ANZAM Conference, Wellington, New Zealand

Cavaliere, L. P. L., Subhash, N., Rao, P. V. D., Mittal, P., Koti, K., Chakravarthi, M. K., Duraipandian, R., Rajest, S. S., & Regin, R. (2021). The Impact of Internet Fraud on Financial Performance of Banks. 12(6).

Chinembiri, T. (2020). Despite reduction in mobile data tariffs, data still expensive in South Africa. Research ICT Africa. Cape Town

Cybercrimes Act, 19 (2020). South Africa

Dan, V. (2019). Empirical and Non-Empirical Methods. Free University of Berlin. Berlin

Deloitte. (2020). Telcos in a post-COVID-19 South Africa. Deloitte Touche Tohmatsu Limited

Denzin, N. K., & Lincoln, Y. S. (2018). The SAGE Handbook of Qualitative Research (Fifth ed.). SAGE Publications.

Detura, R., Ioshiura, C., Murphy, A., Richardson, B., Scheurle, S., Schweikert, E., & Vancauwenberghe, M. (2022). A new approach to fighting fraud while enhancing customer experience. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-new-approach-to-fighting-fraud-while-enhancing-customer-experience

Eitel-Porter, R. (2021). Beyond the promise: implementing ethical AI. *AI and Ethics*, *1*. https://doi.org/https://doi.org/10.1007/s43681-020-00011-6

Elkatawneh, H. H. (2016). COMPARING QUALITATIVE AND QUANTITATIVE APPROACHES. Walden University. Minneapolis, Minnesota

Erin, O. A., Kolawole, A. D., & Noah, A. O. (2021). Risk governance and cybercrime: the hierarchical regression approach. *Future Business Journal*, *6*(12). https://doi.org/https://doi.org/10.1186/s43093-020-00020-1

Floridi, L. (2018). Soft Ethics and the Governance of the Digital. *Phoilosophy & Technology*, *31*, 1-8. https://doi.org/10.1007/s13347-018-0303-9

Floridi, L., & Cowls, J. (2019). A Unied Framework of Five Principles for AI in Society. Harvard Data Science Review, 1.1 Summer, Summer 2019.

Fourie, H. (2019). ETHICS, CULTURES, FRAUD AND CORRUPTION – THE UNANSWERED QUESTIONS. Nelson Mandela University.

Freeman, R. E., Dmytriyev, S. D., & Phillips, R. A. (2021). Stakeholder Theory and the Resource-Based View of the Firm. *Journal of Management*, *47*(7), 1757–1770. https://doi.org/https://doi.org/10.1177/0149206321993576

Fritz, A., Brand, W., Gimpel, H., & Bayer, S. (2020). Moral agency without responsibility? Analysis of three ethical models of human-computer interaction in times of artificial intelligence (AI). *De Ethica. A Journal of Philosophical, Theological and Applied Ethics*, *6*(1).

Gentles, S. J., Charles, C., Ploeg, J., & McKibbon, K. A. (2015). Sampling in Qualitative Research: Insights from an Overview of the Methods Literature. *The Qualitative Report*, *20*(11), 1772-1789. http://nsuworks.nova.edu/tqr/vol20/iss11/5

Graydon. (2020). *External Business Fraud in the UK*. Graydon UK Limited. Middlesex

Halai, A. (2006). ETHICS IN QUALITATIVE RESEARCH: ISSUES AND CHALLENGES Multi Disciplinary Qualitative Research in Developing Countries, , Aka Khan University, Karachi.

Hallamaa, J., & Kalliokoski, T. (2020). How AI Systems Challenge the Conditions of Moral Agency? Culture and Computing : 8th International Conference, Copenhagen, Denmark.

Hanna, R., & Kazim, E. (2021). Philosophical foundations for digital ethics and AI Ethics: a dignitarian approach. *AI and Ethics*, *Volume 1*, 405–423. https://link.springer.com/article/10.1007/s43681-021-00040-9

ICASA. (2022). *The State of the ICT Sector Report of South Africa*. ICASA.

IEEE. (2017). *ETHICALLY ALIGNED DESIGN A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems - Version II*.

IoDSA. (2016). *The King IV Report on Corporate Governance for South African 2016*

Ishak, N. M., & AbuBakar, A. Y. (2014). Developing Sampling Frame for Case Study: Challenges and Conditions. *World Journal of Education*, *4*(3). https://doi.org/10.5430/wje.v4n3p29

Jackson, R. L., Drummond, D. K., & Camara, S. (2007). What Is Qualitative Research? Qualitative Research Reports in Communication, 8(1), 21-28.

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, *1*(9), 389-399. https://doi.org/10.1038/s42256-019-0088-2

Kallio, H., Pietilä, A., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nusirng 72*(12), 2954-2965. https://doi.org/10.1111/jan.13031

Kemp, S. (2020). *FRAUD AGAINST INDIVIDUALS IN THE INTERNET ERA: TRENDS, VICTIMISATION, IMPACT AND REPORTING* Universitat de Gerona]. Spain.

Khadas, H. M. (2020). The Causes of CyberCrime. International Journal of Innovative Science and Research Technology, Volume 5(8).

Li, J. (2023). Analysis on ChatGPT Technology Ethics Governance. *International Journal of Frontiers in Sociology*, *5*(5), 74-77. https://doi.org/10.25236/IJFS.2023.050511

Li, T.-T., Wang, K., Sueyoshi, T., & Wang, D. D. (2021). ESG: Research Progress and Future Prospects. *Sustainability*, *13*, 1-28. https://doi.org/https://doi.org/10.3390/su132111663

Libera, M. (2022, 30 April 2022). South Africa's networks could be forced to collect biometric data — what's next. *MYBROADBEND*. https://mybroadband.co.za/news/cellular/442798-south-africas-networks-could-be-forced-to-collect-biometric-data-whats-next.html

Lubis, F. R., & Hanum, F. (2020). Organisational Culture. *Advances in Social Science, Education and Humanities Research*, *511*.

Mabuza, E. (2021, 25 May 2021). MTN admits identity fraud now a worldwide threat to network operators. *Sowetan Live*. https://www.sowetanlive.co.za/news/south-africa/2021-05-25-mtn-admits-identity-fraud-now-a-worldwide-threat-to-network-operators/

Martinho, A., Poulsen, A., Kroesen, M., & Chorus, C. (2021). Perspectives about artificial moral agents. *AI & EThics*, *1*, 477-490. https://doi.org/doi.org/10.1007/s43681-021-00055-2

Marzuki, M. M., MAJID, W. Z. N. A., AZIS, N. K., ROSMAN, R., & ABDULATIFF, N. K. H. (2020). Fraud Risk Management Model: A Content Analysis Approach. *Journal of Asian Finance, Economics and Business*, *7*(10), 717–728. https://doi.org/doi:10.13106/jafeb.2020.vol7.no10.717

Mišić, J. (2021). Ethics and governance in the digital age. *Wilfred Materns Centre for European Studies*, *20*(2).

Mostafa, A. A. N. (2022). Cyber Crime in Business: Review Paper. *International Journal of Academic Research in Business and Social Sciences*, *12*(6), 962-972. https://doi.org/10.6007/IJARBSS/v12-i6/13865

Müller, V. C. (2021). *The Oxford Handbook of Digital Ethics* (C. Veliz, Ed.). Oxford University Press. https://academic.oüp.com/edited-volüme/37078

Ndlovu, S. (2020). *An investigation of causes of under-reporting of unethical conduct at a Johannesburg Security Exchange listed company*. MANCOSA. Durban

Pasculli, L. (2020). The Global Causes of Cybercrime and State Responsibilities. Towards anIntegrated Interdisciplinary Theory' Journal of Ethics and Legal Technologies, Volume 2(1).

PWC. (2022). PwC's Global Economic Crime and Fraud Survey 2022: Protecting the perimiter - the rise of external fraud. PWC.

PWC. (2023). Future proof your telecommunication workforce today: Telecommunication of the future. PWC.

Rouse, M. (2011, 6 December 2011). Mobile Network Operator. *Techopedia*. https://www.techopedia.com/definition/27804/mobile-network-operator-mno

Ruslin, Mashuri, S., Rasak, M. S. A., Alhabsyi, F., & Syam, H. (2022). Semi-structured Interview: A Methodological Reflection on the Development of a Qualitative Research Instrument in Educational Studies. *IOSR Journal of Research & Method in Education*, *12*(1), 22-29. https://doi.org/10.9790/7388-1201052229

SAFPS. (2023, 17 May 2023). *The SAFPS highlights the need for a proactive approach to fraud prevention at the 2023 Fraud Summit* https://www.fanews.co.za/article/fraud-crime/5/general/1094/the-safps-highlights-the-need-for-a-proactive-approach-to-fraud-prevention-at-the-2023-fraud-summit/37025

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2019). RESEARCH METHODS FOR BUSINESS STUDENTS (Vol. 8). Perason Education Limited.

Schiff, D., Borenstein, J., Biddle, J., & Laas, K. (2020, 7-8 February 2020). What's Next for AI Ethics, Policy, and Governance? A Global Overview Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, New York.

Schoch, K. (2020). Selected research design and approaches. SAGE Publications.

Shava, H. (2021). The relationship between service quality and customer satisfaction in the South African mobile network telecommunications industry. *Journal of International Studies*, *14*(2). https://doi.org/DOI:10.14254/2071-8330.2021/14-2/5

Shukla, S. (2020). *CONCEPT OF POPULATION AND SAMPLE*. Gujarat University. https://www.researchgate.net/publication/346426707_CONCEPT_OF_POPULATION_AND_SAMPLE

Singh, A. (2021). An Introduction to Experimental and Exploratory Research. Patna Women College. Bihar, India

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333-339.

Stahl, B. C. (2022). Responsible innovation ecosystems: Ethical implications of the application of the ecosystem concept to artificial intelligence. International Journal of Information Management, 62 (2022) 102441.

Staller, K. M. (2021). Big enough? Sampling in qualitative inquiry. *Qualitative Social Work*, 1-8. https://doi.org/10.1177/14733250211024516

Stenfors, T., Kajamaa, A., & Bennett, D. (2020). How to assess the quality of qualitative research. *The Clinical Teacher*, *17*, 596–599.

Stubben, S., & Welch, K. (2018). Research: Whistleblowers Are a Sign of Healthy Companies. Retrieved 8 July 2023, from https://hbr.org/2018/11/research-whistleblowers-are-a-sign-of-healthy-companies

Thomas, D. R. (2006). A General Inductive Approach for Analyzing Qualitative Evaluation Data. *American Journal of Evaluation*, *27*(2), 237-246. https://doi.org/10.1177/1098214005283748

Thompson, A. (2022, 20 February 2022). What to do if you're a victim of fraud or a scam in South Africa. *News24*. https://www.news24.com/news24/bi-archive/what-to-do-if-youre-a-victim-of-fraud-or-a-scam-in-south-africa-2022-2

Torkington, S. (2024). These are the 3 biggest emerging risks the world is facing. Retrieved 19 January 2024, from https://www.weforum.org/agenda/2024/01/ai-disinformation-global-risks/

Tracy, S. J. (2010). Qualitative Quality: Eight "Big-Tent" Criteria for Excellent Qualitative Research. *Qualitative Inquiry*, *16*(10), 837-851. https://doi.org/10.1177/1077800410383121

Valentinov, V. (2022). Stakeholder theory and the knowledge problem: A Hayekian perspective. *Business Ethics, the Environment & Responsibility*, *31*(2), 536-545. https://doi.org/https://doi.org/10.1111/beer.12383

Valentinov, V., & Chia, R. (2022). Stakeholder theory: A process-ontological perspective. *Business Ethics, the Environment & Responsibility*, *31*, 762–776. https://doi.org/DOI: 10.1111/beer.12441

Wellard, S. (2022). Digital ethics to support future business innovation. *UK Research & Innovation*. https://www.ukri.org/blog/digital-ethics-to-support-future-business-innovation/

Winfield, A. F., MICHAEL, K., PITT, J., & EVERS, V. (2019). Scanning the Issue. *PROCEEDINGS OF THE IEEE*, *107*(3).

World Economic Forum. (2024). *Global Risk Report 2024.* Retrieved 27 January 2024 https://www.weforum.org/publications/global-risks-report-2024/

Yonder Consulting. (2023). *Online Scams & Fraud Research 2022 Executive Summary Report*. YONDER CONSULTING

APPENDIX A

Interview Guide

Standard Participant Questions

a) What is your role and job level at Company X.
b) How many years have you worked at Company X?
c) What is the division or the functional area that you work in?

Digital Ethics (DE) Governance

1. How is the governance of DE imbedded in the broader governance of ethics in Company X?
2. Who serve on the Digital Ethics Governance Committee (DEGC), and how is the governance of digital ethics conducted in Company X?
3. How is the Social and Ethics Committee (SEC) or the relevant Board Sub-Committee informed on the work performed by the DEGC?
4. How does the DEGC ensure that the use of digital technologies do not cause harm? (That there is a balance between the opportunities and the risks)
5. How does the Company X organisational culture affect the management of DE?
6. How do employees report issues of DE and how are those addressed?
7. How was training conducted to all levels of the employees, to ensure that DE is the responsibility of everyone in Company X?

Digital Ethics Framework

8. What are the digital ethics principles or tenets of Company X?
9. How does the DE framework address prevalent DE risks such as: non-compliance to POPIA, misuse, algorithm bias, poor design, lack of technical skills, lack of quality assurance, incorrect application of the digital technologies and solution?
10. What are the current challenges of DE within Company X?
11. Does the DE framework allow for people of diverse background to be involved in the practical management of DE and are those roles defined? *(For an example, ethics and risk*

professionals to address the ethics and risks issues; the technical professionals to assess the suitability of the technology; the legal professional to assess compliance and legal issues; and business professionals to assess the viability of the solution)

12. How is digital ethics monitored and measured?
13. What are the elements of the DE framework of Company X? *(For example, the prevalent ones are risk management; ethical design; isolation of responsibility; founding principles; compliance to laws; social cost benefit impact analysis; protection of digital assets (cyber and physical); audit trail, post implementation monitoring).*

Digital Fraud Risk Management

14. How are the new digital solutions tested to ensure that they will not weaken the internal controls or enable fraud to be committed?
15. How are the relevant functions (fraud, ethics, compliance and risks) involved before a solution is operationalised and does these functions conduct post implementation assessment to check whether the digital solution is working as intended?
16. What mechanisms are in place to ensure that digital risks are tracked until they have been fully mitigated?
17. How is management setting the right tone in dealing with issues of digital fraud *(committing to address the risk, implementing the recommendations and implementing consequence management)*
18. What processes are in place to ensure that there are consequences for those that commit digital fraud?
19. How are employees, service providers, customers and the public kept informed about the incidences of digital fraud?
20. How does the organisation ensure that it does not prioritise the opportunities (sales generation) derived from digital solutions over the harm that they cause to customers (fraud prevention)?
21. What is the user authentic process to ensure that only authorised individuals have access to Company X digital systems and what are processes available to monitor critical and fraud vulnerable digital systems?

APPENDIX B

Information Participant Sheet

QUALIFICATION	**Masters in Management: Digital Business**

Dear Sir / Madam

1. My name is Simile Ndlovu. I am a Masters degree student in Digital Business at the University of the Witwatersrand (Business School), Johannesburg. My supervisor is Prof. Rene Pellissier. I am conducting a research study about Digital Ethics. The study title is *"The application of digital ethics practices to mitigate digital fraud in a Mobile Network Operator in South Africa"*

2. The background of the study is follows:

   a) As organisations embark on digital transformation, they must embed digital ethics principles and practices to ensure that there is an analysis of both the positives of the digital solutions, and the risks introduced by the same solution. The wide adoption of digital technologies has corresponded with an increase in number of digital fraud cases. The digital fraud in MNO industry is perpetrated by targeting customers or members of the public, and the MNO itself. Other than sabotage and damage to critical network infrastructure, some of the prevalent fraud schemes in MNOs are competition scams, discounted airtime or data scams, sim-swap fraud, porting fraud, post-paid contract application fraud, and various other types of subscription fraud.

   b) The research problem that informs this study is that the risks of digital technologies or solutions are not mitigated due to the lack of adoption of digital ethics practices. This research seeks to explore the application of digital ethics practices to mitigate digital fraud

in Company X. The digital fraud can be mitigated if the upside and downside of technologic solutions are considered. The research problem can be illustrated through the following two examples:

- **Example 1:** Due to a sheer number of transactions below R50. An organisation might design or configure a customer management system to automatically approve all transactions created by an employee that are under R50, that is, they would not require the approval of a manager. The justification from the organisation might be that managers would not have time to look at all the transactions and would rather channel their efforts in much more critical tasks. In the absence of segregation of duties, the digital ethics question is, how would the organisation ensure that customers are not harmed by ensuring that the transactions below R50 are free from manipulation and fraud?

- **Example 2:** In a drive to increase the revenue streams of an organisation, it might decide to offer fintech services. To increase the uptake of their fintech solution, an organisation might decide to design an end-to-end onboarding process that is paperless. The customers can create accounts without submitting the actual copy of their identity documents (ID). This would be a convenience for the customers, and from a business point it might pay-off. The digital ethics question is, what process would be in place to ensure that fraudsters do not harm ordinary members of the public, by opening accounts on the fintech platform using their fraudulently obtained ID numbers?

c) The management of digital ethics must be deliberate act to ensure that the creation of a digital solution to solve one problem, (for an example quick and efficient customer on-boarding), does not create a new problem (for an example, post-paid contract credit application fraud).

3. I am inviting you to take part in a one-on-one interview relating to this study. The participation will last about one hour. The interview will take place online or in person at Company X offices, depending on your preference. The interview will take place during working hours or at a time that is suitable to you.

4. With your permission, I would like to audio record the interview. This data will be stored in a password protected recordable device and will be deleted after two years. Only the researcher will have access to the data.

5. The interview will be confidential and anonymous. When I share the results of the research study, I will not include your name or anything else that could identify you. With your permission, other researchers may use the data collected from this research study, but your name and any personal information will not be used or passed on.

6. The participation in the study is voluntary. You can stop being in the study at any time. You do not have to answer any questions if you do not want to. You will not get any direct benefits if you choose to join the research study. Taking part is free, and you will not be paid for being in this research study.

7. There are no risks to participation either directly to you or your organisation. I trust that you will find it beneficial for you as an individual and for the organisation to participate in this study. Final recommendations based on the research report can be made available to you, if requested.

8. The questions relating to the study can be directed to me or my supervisor on the details listed below. The concerns or complaints about the ethical procedures can be directed to the University Human Research Ethics Committee (Non-Medical), telephone +27(0) 11 717 1408, email hrecnon-medical@wits.ac.za.

Yours sincerely,

Researcher: Simile Ndlovu, 2728774@students.wits.ac.za, 065 822 9119

Supervisor: Prof. Rene Pellissier, rene@pellissier.co.za

APPENDIX C

Participation Agreement (Consent Forms)

<u>Title of project:</u> The application of digital ethics practices to mitigate digital fraud in a Mobile Network Operator in South Africa

<u>Name of researcher</u>: Simile Ndlovu

I, ……., agree to participate in this research project.
I agree to the following:
(Please circle the relevant options below)

The research study was explained to me. I understand what this study is about.	YES	NO
I understand that I can volunteer to take part in the study	YES	NO
I agree that the interview will be audio recorded	YES	NO
I agree that direct quotations from my interview may be used by the researcher in their research report.	YES	NO
I agree that my participation will remain anonymous *(my name or other identifying data will not be used by the researcher in their research report)*	YES	NO
I agree that other researchers may use the information I provide in my interview, but my name and any personal information will not be used or passed on.	YES	NO

…… (Signature)
…… (Name of participant)
…… (Date)

…… (Signature)
…… (Name of researcher)
…… (Date)

APPENDIX D

Permission Letter from Company X

Form Company Wide Resources | REQUEST FOR INFORMATIOM | Group | Human

The name of Company X and other information removed to maintain anonymity.

REQUEST FOR INFORMATION

The High Level Process

In short you need to find an Executive and Subject Matter Expert (SME) in the area you need information and obtain their support and approval.

R - Responsible; A – Accountable; C – Consult with; I - Inform

Steps	Requester	Promoter	Line Executive	HRBP	SME
Need for Information exists. Requester contact HRBP for advise	R	I		C	
Requester to complete approval form	R/A	I		C	
Line Executive approves/do not approve	I	I	R/A	I	I
Line Executive informs the Requester of outcome	I	I	R/A	I	I
SME provides information through a discussion session	A	I	I	I	R

REQUEST FOR INFORMATION

NAME OF RESEARCHER: Simile Ndlovu

SERVICE ORGANISATION: Corporate

SALARY REF NUMBER: 4509403

JOB TITLE & LEVEL: Executive: Forensics

PROMOTER: [redacted]

E-MAIL: [redacted]

TELEPHONE NUMBER: 0658229119

STUDY INSTITUTION: Wits University

LECTURER/ STUDY LEADER/ Professor Rene Pellissier

Description of the research topic	**An assessment of digital ethics framework and governance practices to mitigate digital fraud in a Mobile Network Operator in South Africa**
Information Required	The permission to conduct interviews with selected employees (between 8 and 13). The employees will in function relates to the study, specifically those in Fraud, Risk, Ethics, and those that design digital solutions or implement digital technologies. Secondly access to documents policies, procedures and any other information related thereto for the purpose of documents review. It should be emphasized that the organisation name or any identifying feature will be in the final report. For that specific reason, the organisation will be referred to as Company X
Purpose of information	To fulfil the requirements of a qualitative research study, for a master's degree in Digital Business at Wits Business School (WBS). It should be noted this study is funded by the organisation through a bursary
How will the information be used?	The collected data is for academic purposes, and nothing else. As indicated no name or identifying feature of the organisation will be mentioned in the final dissertation. As is the case with all qualitative academic studies, the participants (those that will be interviewed) will remain anonymous
Who will have access to this information?	Only the researcher (myself) and the academic supervisor, Professor Rene Pellissier
Where will the research project/assignment be published	The final master's degree dissertation will be published on the Wits University online library. There is no risk to the organisation as there will be nothing therein that identifies the organisation.

FOR OFFICIAL USE – TO BE COMPLETED BY HR BUSINESS PARTNER IN CORPORATION WITH SME AND LINE EXECUTIVE

Process A

SO where research will be conducted: Telkom SOC	
Name: SME (Subject Matter Expert)	[redacted]
Name: HR Business Partner	[redacted]
Recommendation (Yes) Line Executive	
Reason Technology/Digitisation	**The research will assist with understanding the impact of on key assurance functions (i.e., risk, fraud and ethics)**
Information that will be provided?	Permission for conducting interviews with the selected individuals, only for the purpose of the study, for primary data collection
Date	**13 July 2023**
Signature	
Approved By: (Line Executive)	[redacted]
Date	**13 July 2023**

APPENDIX E

University Ethics Approval

Graduate School of Business Administration
University of the Witwatersrand, Johannesburg

Wits Business School Ethics Committee
Constituted under the University Human Research Ethics Committee (Non-Medical)

Ethics Clearance Certificate

Ethics protocol number: WBS/DB2728774/453
This certificate is only valid with a legitimate ethics protocol number and signed by the Researcher (below)

Project title	The application of digital ethics practices to mitigate digital fraud in a mobile network operator in South Africa
Investigator / Researcher	Mr Simile Ndlovu
Nature of Project	MM (Digital Business)
Decision of the Committee	Approved, provided stakeholders and participants are guaranteed confidentialty.
Issue Date of Certificate	2023/10/17
Expiry date	Date of submission of the project / research report
Chairperson	Dr Pius Oba ☎ +27 11 717 3976 +27 82 733 6587 pius.oba@wits.ac.za

Declaration by Researcher

One copy must be signed by the Researcher and returned to the Chairperson of the Wits Business School Ethics Committee.

I fully understand the conditions under which I am authorized to carry out the abovementioned research and I guarantee to ensure compliance with these conditions. Should any departure to be contemplated from the research procedure as approved I undertake to resubmit the protocol to the Committee.

Signature

17 October 2023
Date:

ANNEXURE F

Turnitin First Page