

A digital fraud strategy framework for banks and insurance companies in South Africa.

Applied Research Project

Submitted by

Nonhlanhla Mahlangu

Student number: 1168252

Tel: +27 76 319 4461

Email: nhlaksmahlangu@gmail.com

Supervisor:

Dr Oro Ufuo Oro

Wits Business School

[March 2022]

Table of Contents

LIST OF FIGURES AND TABLES	iv
DECLARATION	v
DEDICATION	vi
ACKNOWLEDGEMENTS	vii
ABSTRACT	viii
CHAPTER ONE: INTRODUCTION	1
1.1 CONTEXT OF THE STUDY.....	1
1.1.1 Digital platforms.....	2
1.1.2 Types of digital fraud.....	2
1.2 PROBLEM STATEMENT	3
1.2.1 Research problem	3
1.2.2 Research objectives.....	4
1.2.3 Research questions	5
1.3 SIGNIFICANCE.....	5
1.4 DELIMITATIONS	5
CHAPTER TWO: LITERATURE REVIEW	6
2.1 INTRODUCTION	6
2.1.1 The fraud triangle theory	6
2.1.2 The fraud diamond theory.....	8
2.3 DEFINITION OF TERMS.....	9
2.3.1 Cybercrime	10
2.3.2 Cyber fraud.....	10
2.3.3 Digital fraud	10
2.4 THEORETICAL FRAMEWORKS.....	11
2.4.1 Legislation and regulations	11
2.4.2 Technology	11
2.4.3 Education and awareness.....	12
2.5 CONCEPTUAL FRAMEWORKS.....	12
2.5.1 Conceptual framework for digital fraud knowledge management.....	12
2.5.2 Conceptual framework for digital fraud risk management in banking	13
2.5.3 Big data analytics on combating cyber fraud	15
2.6 CONCLUSION OF LITERATURE REVIEW	16
2.6.1 Theoretical frameworks	16

2.6.2 Conceptual frameworks.....	17
CHAPTER THREE: RESEARCH METHODOLOGY	18
3.1 RESEARCH METHOD	18
3.2 RESEARCH DESIGN	18
3.3 RESEARCH APPROACH	19
3.4 UNIT OF STUDY	19
3.5 POPULATION	19
3.6 SAMPLE SIZE.....	20
3.7 DATA COLLECTION PROCESS	20
3.7.1 Ethics.....	21
3.7.2 Informed consent.....	21
3.8 ANONYMITY AND CONFIDENTIALITY	21
3.9 VALIDITY AND RELIABILITY	22
CHAPTER FOUR: PRESENTATION OF THE RESULTS	23
4.1 QUANTITATIVE DATA ANALYSIS.....	23
4.1.1 Descriptive quantitative dataset	23
4.1.2 Evaluate a digital fraud strategy framework for banks and insurance companies in South Africa.....	26
4.1.3 Data coding	29
4.1.4 Diagnostic test statistics	31
4.1.5 Regression estimations	31
4.1.6 Robustness checking.....	33
4.1.7 Conclusion on quantitative analysis	35
4.2 QUALITATIVE DATA ANALYSIS.....	36
4.2.1 Descriptive qualitative dataset.....	37
4.2.2 Organisational structure	38
4.2.3 Legislation and regulations	40
4.2.4 Strategy.....	42
4.2.5 Technology	43
4.2.6 Forensics	45
4.2.7 Education and awareness.....	46
4.2.8 Data and analytics.....	48
4.2.9 Conclusion on qualitative analysis.....	50
CHAPTER FIVE: DISCUSSION OF THE RESULTS	51
5.1 Introduction	51

5.2 Legislation and regulations.....	51
5.3 Education and awareness	52
5.4 Organisational structure.....	54
5.5 Technology	54
5.6 Big data and analytics	55
5.7 Investigations.....	56
5.8 Strategy	57
5.9 The digital fraud strategy framework	58
CHAPTER SIX: CONCLUSION.....	62
6.1 Introduction	62
6.2 Research objectives	62
6.3 Policy suggestions	63
6.4 Suggestions for future research	64
REFERENCES	66
APPENDICES.....	70
Appendix 1: Survey	70
Appendix 2: Interview Guide	82
Appendix 3: Ethics Clearance Certificate	85
Appendix 4: Participant Consent Information (Online Survey)	86
Appendix 5: Participant Consent Information (Interviews)	87
Appendix 6: Participant Consent Form (Interviews).....	88
Appendix 7: Correlation Matrix.....	89
Appendix 8: Cross-functional Team	90
Appendix 9: Fraud Policy Documents	91
Appendix 10: Ethical Policy Document, Fraud Prevention Policy.....	92
Appendix 11: Fraud Prevention Policy.....	92
Appendix 12: Digital Intelligence Responses.....	93
Appendix 13: Responses on Behavioural Biometrics	94
Appendix 14: Responses on In-App Messaging.....	95
Appendix 15: Responses on Personal Identification Information	96

LIST OF FIGURES AND TABLES

Figure 1: The fraud triangle	7
Figure 2: The fraud diamond	9
Figure 3: Conceptual framework for digital fraud knowledge management.....	13
Figure 4: Conceptual framework for digital fraud risk management in banking	14
Figure 5: The Five V model of big data.....	15
Figure 6: Position levels held by respondents	24
Figure 7: Banking and insurance composition	24
Figure 8: Skills set variations of the respondents	25
Figure 9: Distribution of roles and duties of the participants' interviewed	37
Figure 10: Department functions of the interview participants	38
Figure 11: Defined roles and responsibilities	40
Figure 12: Summary of responses on cyber digital policy documents.....	41
Figure 13: Percentage of earning losses due to digital fraud	43
Figure 14: Responses regarding the use of AI	44
Figure 15: Responses on forensic or investigation department	46
Figure 16: Education and awareness campaigns, external.....	47
Figure 17: Big data to prevent digital fraud.....	49
Figure 18: A digital fraud strategy framework for banks and insurance companies	60
Table 1: Percentage share of the position set of the respondents	25
Table 2: Variables' description	27
Table 3: Summary statistics	29
Table 4: SPSS regression coefficients estimation model-1.....	33
Table 5: SPSS regression coefficients estimation model-2.....	34
Table 6: SPSS regression coefficients estimation model-3.....	35

DECLARATION

I, Nonhlanhla Mahlangu, declare that this research project 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 Business Administration in the Graduate School of Business Administration, University of the Witwatersrand, Johannesburg. It has not been submitted before for any degree or examination in this or any other university.

Signed at

On the day of 20.....

DEDICATION

I dedicate this research to my son, Mikhenso Nkwana.

My grandmother, Sesana Chili, thank you for always believing in me, for your support and for your guidance.

My mother, Sarah Mahlangu, thank you for the opportunities you have provided me with, for your love, support, and your guidance.

ACKNOWLEDGEMENTS

I am very grateful to God for providing me with the strength that I needed to successfully complete this research, and for all of the opportunities that He continues to bless me with, I will forever be grateful.

A big thank you to my supervisor, Dr Oro Ufuo Oro, for all his assistance and guidance throughout my research journey.

I would like to acknowledge my good mentor, Lunga Siyo. Thank you for encouraging me to further my studies. I would not have walked this journey if it had not been for the role you played in guiding me on the right path.

My two amazing sisters, Naledi and Mbali, deserve a heartfelt thank you for always being there for me when I needed them. Nothing feels better than knowing that I can rely on you. You are greatly appreciated.

Thank you to my employer, Old Mutual, for the support they have given me during my MBA journey.

Thank you to all my friends and family for their support during my MBA.

ABSTRACT

South African banks and insurance companies have been focused on transforming and accelerating their digital strategies. There has been much focus for most organisations on providing products or services across various digital platforms. As a result, fraudsters are also finding new ways to commit fraud on the same digital platforms. Consequently, digital fraud numbers have increased, and banks and insurance companies should ensure that they implement suitable measures that will help them predict, prevent, detect, monitor, and respond to digital fraud in real time while protecting their customers' financial goals and improving customer experience.

Existing studies have revealed components of combating digital fraud for the South African financial service providers, but no study on a holistic digital fraud strategy framework has been conducted. The aim of this research is therefore to evaluate a digital fraud strategy framework for South African banks and insurance companies, and to obtain a better understanding of how to combat digital fraud for South African banks and insurance companies.

A mixed-methods approach was used in this study, in which participants in the banking and insurance industry were surveyed, and digital fraud subject matter experts were interviewed.

Data analysis revealed that organisational structure, education and awareness, policies, big data, and analytics all have an impact on reducing digital fraud for South African banking and insurance institutions. The study also found that government legislation does not affect the reduction of digital fraud. South African banking and insurance institutions therefore need to implement appropriate measures that will help combat digital fraud.

Keywords:

Digital fraud; cyber fraud; fraud management; digital fraud strategy framework; digital platform; predict fraud; prevent fraud; detect fraud

CHAPTER ONE: INTRODUCTION

1.1 CONTEXT OF THE STUDY

On a global scale, the financial services sector in South Africa is well recognised and highly competent. For 2016/2017, the sector ranked number 11 out of 136 countries for financial sector development. Banks, in particular, are consistently ranked among the world's best (Bernstein, et al., 2017). The South African Fraud Prevention Services (SAFPS) released the 2020 fraud statistics, which indicated significant increases in key aspects such as impersonation fraud (337 percent), fraud listings (62 percent), and victim listings (54 percent). The COVID-19 pandemic played a role in accelerating digital adoption, as most of the financial services sector embraced digital transformation in South Africa. While the financial services sector embarked on a digital transformation journey, fraudsters also created new opportunities to defraud customers and the fraud numbers continue to increase in the financial services sector (SAFPS, 2021). Leading financial service providers adopt critical methodologies to predict, prevent, detect, and monitor fraud based on global benchmarks, best practices, and fraud risk assessments. Equally so, it is critical for the financial industry, specifically banks and insurance companies, to establish a digital fraud strategy that incorporates big data, technology, and knowledge transfer to combat digital fraud.

The South African Banking Risk Information Centre (SABRIC) reported that digital banking fraud incidents increased by 20 percent across all platforms in 2019 compared to 2018, resulting in an increase of 8 percent in gross loss (Maluleke, Motseki, Mokwena, & Dlamini, 2021). Banks in South Africa anticipate increased cybercrime trends because they have been exposed to it, whereas insurance companies have not been significantly impacted historically but are now also impacted (Herselman & Warren, 2004). The financial services industry in South Africa is a highly competitive environment where the industry's market position heightens its competitiveness with changing demographic, technological and customer preferences. If banks and insurance companies are unable to anticipate and respond to these pressures and effectively compete and mitigate associated

fraud risks, their business, financial condition, results of operations, and prospects will suffer substantially.

Most financial companies are accelerating their digital strategies and, as a result, digital adoption is increasing, and fraudsters are also finding new ways of defrauding digital customers. While it is essential for financial companies (specifically banks and insurance companies) to focus on digital transformation and digital acceleration, it is even more critical for banks and insurance companies to set up digital fraud capabilities that will predict, prevent, detect, monitor, and respond to digital fraud in real time. To implement a digital fraud strategy framework, banks and insurance companies need to adopt an approach that looks at an entire customer life cycle and is strategically driven by the entire group.

1.1.1 Digital platforms

Different types of digital platforms enable digital fraud:

- Mobile applications, which can be downloaded from a variety of online application stores.
- Secure online platforms accessible through websites using login or account credentials.
- A mobile platform, which can be accessed through Unstructured Supplementary Service Data (USSD), a digital platform interface that facilitates USSD communication between a service provider such as banks and mobile network operators. It operates on black-and-white cellphones, as well as smart phones and feature phones.
- WhatsApp, a digital platform that has recently been introduced in South Africa's financial industry for performing transactional activities such as submitting claims, disinvestments and retrieving policy documents.

1.1.2 Types of digital fraud

Phishing scams, vishing, email hacking and business email compromise are the most common types of digital banking fraud. Phishing scams involve fraudulent

emails sent to customers in order to obtain valuable information such as Personal Information Numbers (PINs), passwords, one-time passwords, and account numbers. In some cases, fraudsters use SIM swap to take control of a customer's device and gain access to banking apps, allowing them to start making card-not-present (CNP) transactions. Vishing is a type of fraud in which fraudsters use phone calls or voice messages to obtain valuable information from customers.

1.2 PROBLEM STATEMENT

1.2.1 Research problem

Digital fraud is on the rise in South African banks and insurance companies.

Existing research reveals that many financial institutions worldwide are attempting to develop fraud capabilities that will improve digital fraud (Ahmed, et al., 2021). Studies revealed that cybercrime costs South Africa approximately R2.65 billion each year (Chitimira & Ncube, 2021). Another study shows that South African financial companies face significant challenges in combating fraud, with a lack of legislation identified as a major issue (Dzomira, 2015). According to another research study, South African banking and insurance institutions are faced with a fundamental problem when it comes to digital fraud, and a lack of regulations appears to be a huge issue.

Existing studies also found that knowledge management helps South African banks to prevent digital fraud but highlight the need for fraud prevention strategies and policies to be conducted further in the research field (Barker, 2020). The study on knowledge management in South African banks does not address the research problem, however, it highlights a fundamental issue relating to digital fraud, and a need to conduct further studies on digital fraud strategies. Therefore, this study will also explore aspects of the key issues highlighted from the knowledge management study. If the issues raised were not addressed, it therefore means that the solutions to the problems were not found. There is a need to explore a digital fraud strategy framework to address the research problem.

According to SABRIC, fraudsters are exploiting customers on digital platforms, which is attributed to the development of digital technologies. The number of reported digital fraud incidents increased by 64 percent in 2018 (SABRIC, 2021).

1.2.2 Research objectives

The primary objective of this study is to evaluate a digital fraud strategy framework for South African banks and insurance companies in order to obtain a comprehensive understanding of a practical digital fraud strategy framework for South African banks and insurance companies.

The secondary objective of this study is to assess factors that impact digital fraud in banks and insurance companies in South Africa, and to evaluate the impact of digital fraud legislation and regulations for banks and insurance companies in South Africa.

In addition, the study aims to contribute to the research theory, practice, and subsequent academic research, which other students, researchers or professional leaders who are interested in the study of digital fraud in the field of banking and insurance in South Africa can use. A study conducted by Rachel Barker revealed that fraud prevention strategies and policies are needed in the South African financial sector (Barker, 2020).

It is essential for banks and insurance companies to adopt a strategic framework in response to both internal and external factors, including a refresh of technology platforms, digital initiatives, and other strategic projects to help mitigate digital fraud. If a strategic framework is not successfully implemented or associated risks are not managed effectively, it will hurt the business, reputation, and operations.

1.2.3 Research questions

1. What is a practical digital fraud strategy framework for banks and insurance companies in South Africa?
2. What factors impact digital fraud in banks and insurance companies in South Africa?
3. What impact does digital fraud legislation and regulations have on South African banks and insurance companies?

1.3 SIGNIFICANCE

The research will fundamentally add value in research studies on digital fraud in the field of banking and insurance in South Africa. The study will provide a digital fraud strategic solution for the banking and insurance business in South Africa. The study will help the mentioned groups to realise the following about digital fraud in the banking and insurance sector:

- A practical digital fraud strategy framework for South African banks and insurance companies.
- Factors that impact digital fraud for South African banks and insurance companies.
- The impact of digital fraud legislation and regulations for South African banks and insurance companies.

1.4 DELIMITATIONS

The information used in this research study will focus on fraud that takes place on digital platforms in South African banks and insurance companies only. The information on cybercrime and cyber fraud within the banking and insurance industries will also be used as it is relevant to the study. However, cybercrime and cyber fraud are very broad. Therefore, the study will be narrowed down to cybercrime and cyber fraud information related to digital platforms within the banking and insurance space. Other aspects of cybercrime or cyber fraud that might affect banks and insurance companies as a whole will not be included in this study.

CHAPTER TWO: LITERATURE REVIEW

2.1 INTRODUCTION

This section will discuss key concepts of the research topic and relevant research previously conducted in the financial industry, specifically for banks and insurance companies in South Africa. As financial industries move towards digital transformation to meet customers' financial needs through their preferred digital platforms, fraudsters are also finding new ways to defraud customers. Many financial companies are accelerating their digital strategies by introducing convenient digital platforms such as WhatsApp, USSD and other digital platforms to perform transactions. South African banks are under pressure to transform their business model in order to remain relevant to a customer-centric approach (Ronnie & Ditshego, 2020). It is very critical for financial companies to build digital fraud capabilities that will protect their customers from digital fraudulent activities. The financial sector is far more sophisticated than other industries when it comes to digital safety issues (Dzomira, 2015).

Financial institutions are beginning to offer more banking solutions on digital platforms, and the provision of digital services poses a risk to the bank because digital fraud can be performed on the same digital platform (Dzomira, 2015).

Digital fraud is increasing at an exponential rate as fraudsters create new and more sophisticated tactics to target and exploit people for financial gain (Drew & Farrella, 2018).

2.1.1 The fraud triangle theory

In a research study on fraud, Donald Cressey argued that people's actions almost always have a motive behind them (Abdullahi & Mansor, 2015). Donald Cressey's study, in which he conducted interviews with 250 fraudsters in 1950 over a five-month period, found that three factors are usually present for an offense to occur, and that fraud is most likely caused by a combination of these three factors. Figure

1 below shows the fraud triangle model, which is made up of a combination of motivation, rationalisation, and opportunity.

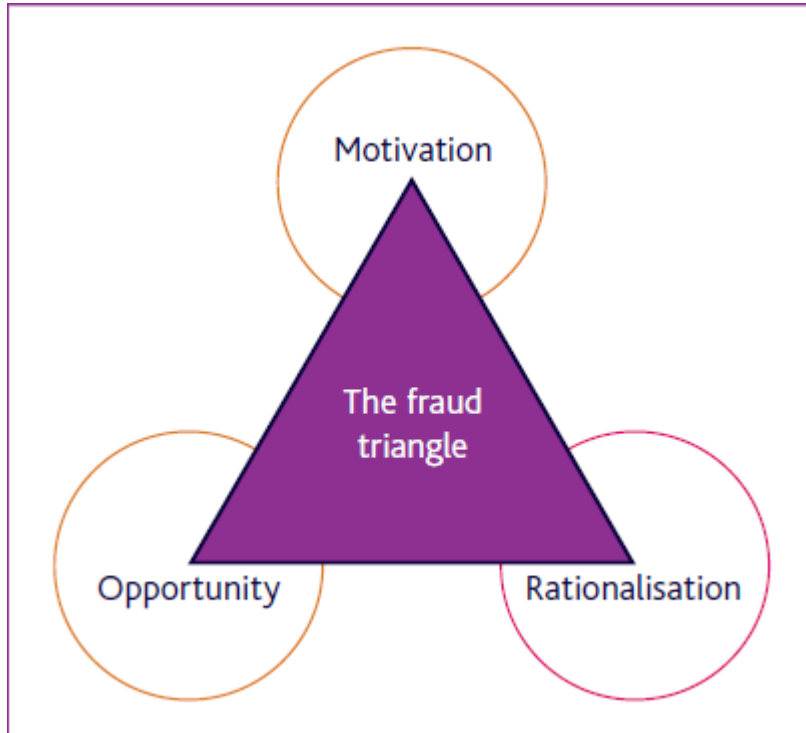


Figure 1: The fraud triangle
Source: (CIMA, 2009)

According to a FraudTrack survey, greed remains the most common reason for fraud, accounting for 63 percent of fraud incidents reported in 2007 (CIMA, 2009). Problems with debts and gambling were also mentioned in the FraudTrack study. At some point, every fraudster feels compelled to act unethically (Abdullahi & Mansor, 2015). Financial pressure is the most common element that leads to an entity engaging in unethical behaviour. Pressure can take place in a number of ways, especially when there are no resources to share a financial need. The perception of opportunity is another crucial component of the fraud triangle. An ineffective control and/or governance structure creates an opportunity for individuals or entities to commit corporate fraud. According to the concept of perceived opportunity, people will take advantage of available conditions (Abdullahi & Mansor, 2015). Fraud is more common in companies that lack internal control systems and have inadequate security over corporate assets, a low fear of exposure and detection, and unclear policies concerning unethical conduct. Research shows

that some employees are completely honest and transparent, while others are completely dishonest, and many are influenced by opportunities (CIMA, 2009). Generally, the lower the risk of being caught, the more likely fraud will occur. Fraud perpetrators are more likely to commit fraud if there is an ineffective management division, a lack of internal controls or systems, and irregular auditing. The reasons and excuses that differentiate unethical behaviour from illegal activity are referred to as the rationalisation element. It is uncommon that a person will commit fraud if they cannot justify their unethical behaviour. Since it is difficult to comprehend the mind of a fraud perpetrator, rationalisation is challenging to detect. Rationalisation is the rationale behind a fraudulent action that people use to justify the necessity and justification on the part of a fraud perpetrator (CIMA, 2009).

Implementing measures that reduce opportunities and motivations for fraudulent actions is an effective way to reduce fraud risk. As discussed in the above section of the triangle of fraud, it is important for companies to have suitable measures in place that will combat fraud. Clear policies, effective processes and systems, and regular risk assessments or auditing are some of the important measures that companies should implement.

2.1.2 The fraud diamond theory

Since the introduction of the fraud triangle theory, the nature of fraud has evolved. A study by Wolfe and Hermanson (2004) argued that the element of capability also plays a role when a person or entity commits fraud. Accordingly, Wolfe and Hermanson added a new element to the fraud triangle theory, namely capability. The element of capability refers to the skills set or capacity required to commit fraud. Figure 2 below depicts the four elements of the fraud diamond.

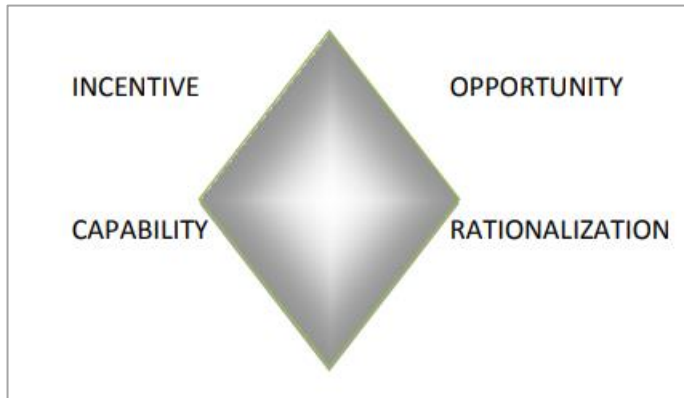


Figure 2: The fraud diamond
Source: (Wolfe & Hermanson, 2004)

Based on Wolfe and Hermanson, an employee or a function in a company has the ability or the skills to create measures that can prevent fraud, but the same employee or business function can create an opportunity for fraudulent activity to occur (Wolfe & Hermanson, 2004).

Recent studies emphasise the importance of embedding employees' ethical values (Mohottige, et al., 2018). Several studies have emphasised that ethical standards among employees lower the likelihood of company fraud. Using a top-down strategy, a tone should be set at the top to instil an ethical culture among the employees.

Most organisations have evolved in how they conduct business, and the financial industry is no exception. Banks and insurance companies have developed processes and systems that enable customers to conduct banking transactions or insurance services digitally.

2.3 DEFINITION OF TERMS

It is important to define key concepts related to the study before commencing a literature review on digital fraud. The section below defines cybercrime, cyber fraud and digital fraud.

2.3.1 Cybercrime

Specific definitions of cybercrime are still being debated, but two major categories are commonly recognised (Drew & Farrella, 2018). The first category includes fraudulent activities involving computers or related Information Technology (IT) and these fraudulent activities take place in the online environment. The second category includes fraudulent activities in which computers or related IT are used to commit crimes. These fraudulent activities relate to customary crimes that are made easier or facilitated by the use of the internet (Drew & Farrella, 2018). Cybercrime is defined as any illegal activity in which a computer, system and/or hardware device is used as a facilitator of a crime (Chitimira & Ncube, 2021). Cybercrime relates to crimes committed using a computer or technology, although murder can also be referred to as cybercrime (Herselman & Warren, 2004). For example, an individual who disrupts a train while conducting a criminal offense that affects a train network and results in the deaths of passengers is considered a cybercrime.

2.3.2 Cyber fraud

Cyber fraud is defined as crimes targeted at computers or Information and Communications Technology (ICT) such as unlawful admission of information and they are carried out in order to obtain a financial gain (Drew & Farrella, 2018). Electronic fraud is also known as cyber fraud, and it is classified into two types: direct and indirect cyber fraud. Cards and money laundering are examples of direct cyber fraud. Phishing is an example of indirect cyber fraud.

2.3.3 Digital fraud

Any fraud that involves a computer or digital device and a network is referred to as digital fraud (Dzomira, 2015). According to Radware (2021), Digital fraud is “the use of a computer for criminal deception or abuse of web-enabled assets that results in financial gain”.

For the purposes of this study, the focus will be on digital fraud or cyber fraud. Digital fraud and cyber fraud will be used interchangeably.

2.4 THEORETICAL FRAMEWORKS

This section of the literature review focuses on the theoretical frameworks used for the study. A theoretical framework is used to structure a study's theory, explore additional information, and reveal links between unrelated topics (Dziak, 2020).

2.4.1 Legislation and regulations

Digital fraud is regulated under cybercrimes, which is prohibited in the country under both the Electronic Communications and Transactions Act (ECTA) and Common Law. Neither of these laws have been effective in combating digital fraudulent activities in South Africa. The ECTA, Common Law, and the National Cybersecurity Policy Framework were implemented in 2015 to combat cybercrime in South African financial institutions (Chitimira & Ncube, 2021). South Africa recently introduced a cybercrime bill that has yet to be enacted into law; however, Chitimira and Ncube argue that it will be ineffective for South African financial institutions because its measures do not include usage of Artificial Intelligence (AI), fifth generation (5G) network technology and other technological measures (Chitimira & Ncube, 2021). The development and implementation of stringent policies, such as consumer education and awareness, systems and strategy, can mitigate many of the digital fraud risks associated with identity fraud in the banking industry (Dzomira, 2015).

2.4.2 Technology

An existing study shows that as banks and insurance companies implement technological innovations to accelerate their digital strategies and drive digital platform adoption, opportunities for digital fraud become more evident (Bernstein, et al., 2017). The banking industry has a critical role in the economic development and growth of any nation. Information and Communications Technology is everywhere, and digitisation is growing at a fast pace and it is becoming more critical to protect banks from digital fraud. Fraudsters use the same ICT systems that banks use for financial gain (Dzomira, 2015). There is an increasing need to focus on self-defence as the number of digital fraud cases grows (Drew & Farrella,

2018). It is critical for banks to remain extra cautious against fraudsters who take advantage of the banking system's flaws and weaknesses. Digital fraud victims must be able to identify their risk, understand the strategies required to combat digital fraud and also understand how they are profiled as suitable targets through usage of their digital platforms, and they should have the technological capabilities to implement preventative measures (Dzomira, 2015). One of the most effective methods to prevent fraud before it can cause a negative financial impact to banks and insurance companies is to use technology that has been proven to prevent it, particularly in digital banking and payments, as this is one of the most effective methods to prevent it before it causes any damage (Entersekt, 2021). Digital fraud can be reduced by implementing relevant technologies such as robust authentication systems and analytics tools (Bhasin, 2016).

2.4.3 Education and awareness

Customer education and awareness are the most effective ways to prevent digital fraud (Dzomira, 2015). It is critical to keep customers informed about the risks of digital fraud at all times, as it helps customers know what to look out for. Customers are more at ease when banks can demonstrate that they have taken proactive steps to secure their digital platforms and constantly assess their solutions to prevent and detect fraud (Entersekt, 2021). Banks must make security and safety information about digital banking available on their websites and other digital platforms (Dzomira, 2015). According to SABRIC, financial companies need to communicate with customers to ensure that they obtain the most up-to-date information regarding digital fraud (Barker, 2020). Customers must also take responsibility for the information provided by SABRIC and recognise that transparency, recommended initiatives, and policies will affect them when they are impacted (Barker, 2020).

2.5 CONCEPTUAL FRAMEWORKS

2.5.1 Conceptual framework for digital fraud knowledge management

SABRIC provides the public with the latest information on banking crimes on their website to create awareness. SABRIC represents the major banks in South Africa.

The conceptual framework in Figure 3 focuses on driving digital fraud awareness to prevent fraud risk and uses three key elements: knowledge acquisition, knowledge transfer and knowledge assimilation. Knowledge acquisition refers to new fraudulent activities that customers can expect in the banking industry and how they should respond to suspicious fraudulent activities. When fraudsters obtain access to customers' accounts, customers are frequently notified through using a security centre website and anti-fraud software pop-ups. Knowledge transfer refers to fraud content that is constantly created and updated on a regular basis. Different messages and links enable banks and customers to collaborate and share information in real time online. Controlling and managing information during and after a fraudulent activity is referred to as knowledge assimilation (Barker, 2020).

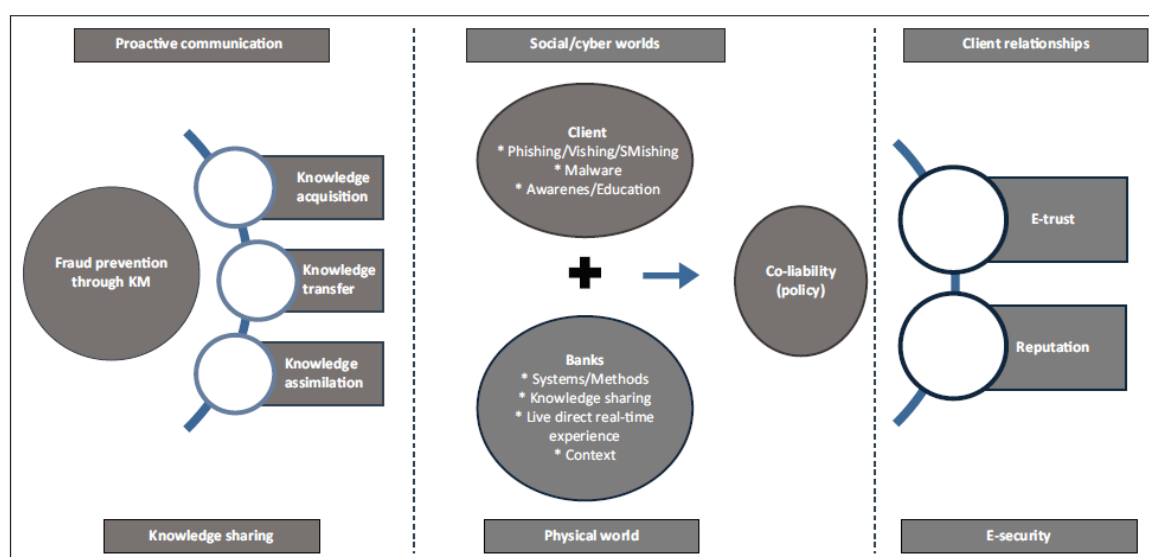


Figure 3: Conceptual framework for digital fraud knowledge management
Source: (Barker, 2020)

2.5.2 Conceptual framework for digital fraud risk management in banking

Financial institutions need to be alert, as with every feature or service that is launched on digital platforms, there are always new fraud risks associated with it (Dzomira, 2015).

The concepts necessary for a more practical approach to digital fraud risk management include the environment, fraudsters, victims, and the guardian (banks), as depicted in Figure 4. Every person in the system is affected by legislation and regulations, technology, education and awareness, governance, and risk management.

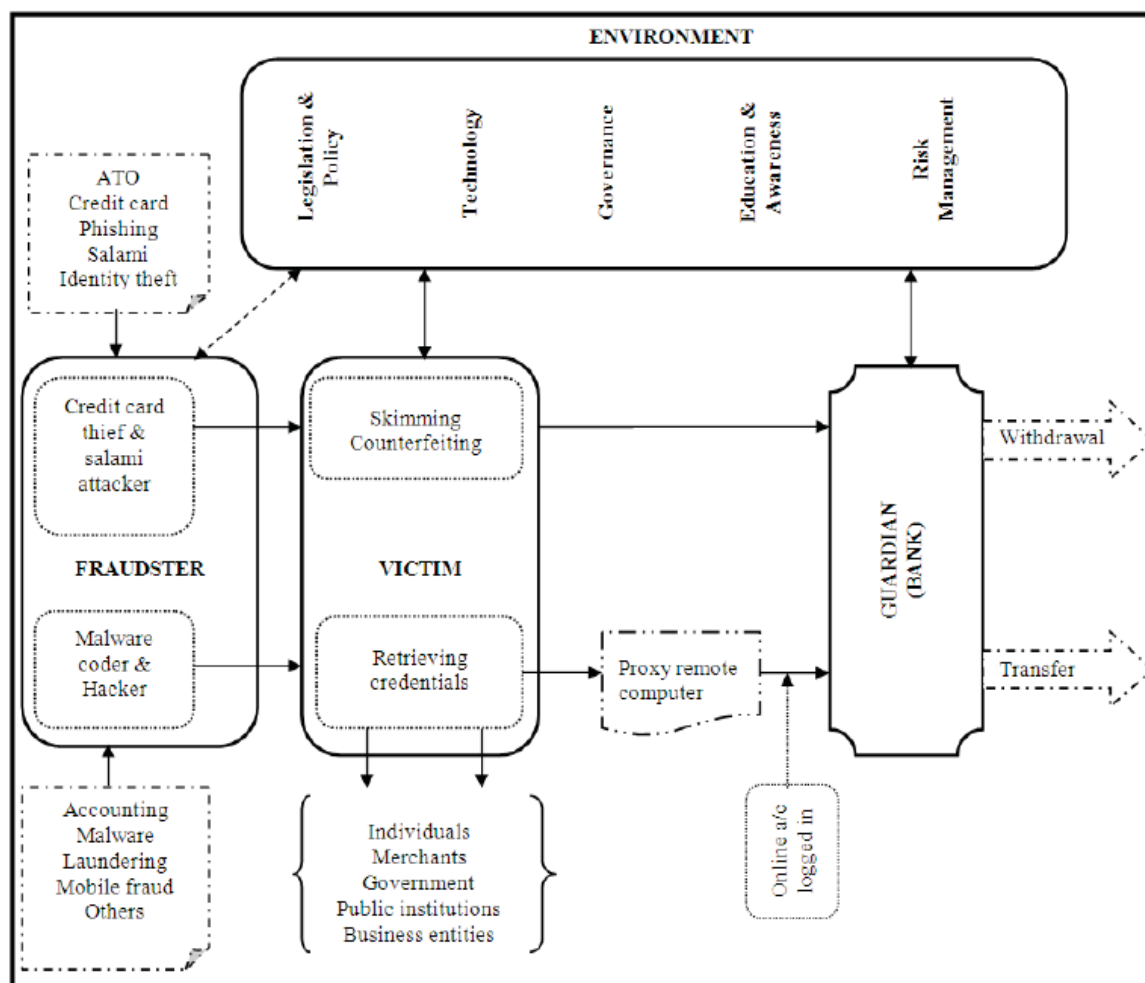


Figure 4: Conceptual framework for digital fraud risk management in banking
Source: (Dzomira, 2015)

Shewangu Dzomira (2015) proposes a conceptual framework for digital fraud risk management in banking, suggesting that an effective digital fraud framework can be effective if all of the different components are employed together rather than separately to prevent digital fraud. The different components in the framework include fraudsters, victims (clients), the bank and the environment. The environment which has an impact on everyone in the model is made up of five

factors, namely: legislation and policy, technology, governance, education and awareness, and risk management. The study acknowledges that the model is weakened by the fact that legislation varies by country, which could pose a problem if digital fraud is committed between countries.

The conceptual framework for digital fraud risk management in banking does not include big data under environment, which is also important for preventing, detecting, predicting, monitoring, and responding to fraud through data. Big data can also be used for predictive analytics capability that proactively identifies digital fraudulent activity as early as possible, with minimal disruption to business decision-making or customer experience.

2.5.3 Big data analytics on combating cyber fraud

"Big data" refers to the development and application of technologies that allow the right user to receive the right information at the right time from a massive amount of data that has been growing exponentially for a long time. The challenge is not only dealing with rapidly increasing data volumes, but also dealing with increasingly diverse forms of sophisticated and interconnected data (Riahi & Riahi, 2018). The three concepts of the five V's are volume, variety, velocity, veracity, and value, as depicted in Figure 5 below.

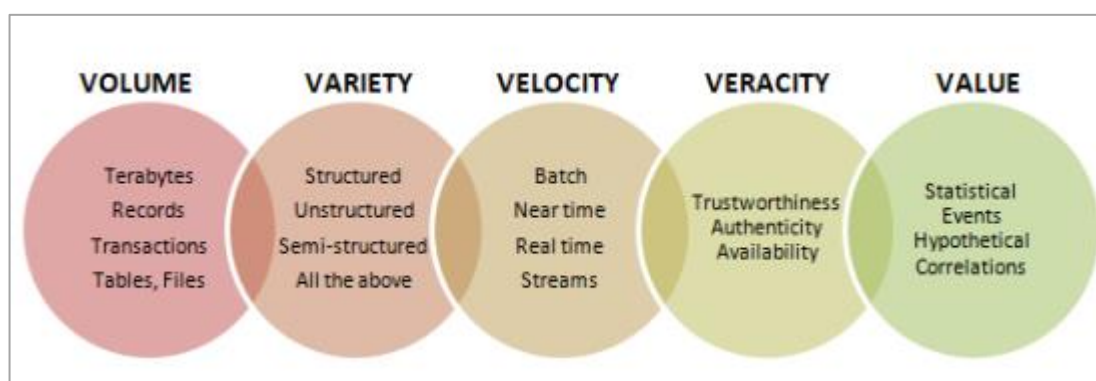


Figure 5: The Five V model of big data
Source: (Riahi & Riahi, 2018)

Volume denotes the amount of data generated, saved, and used by the system. Variety indicates the multiplication of the sorts of data that an information system

can manage. The frequency with which data is created, collected, and exchanged is referred to as velocity. The data is collected in the form of a stream, which must be processed in real time. The degree to which data and data sources are of good or bad quality, unreliable or reliable, is referred to as veracity. The value and potential extracted from data is referred to as value (Riahi & Riahi, 2018).

Following the discussion of big data is big data analytics, which is more concerned with obtaining insights from big data. A study by Eulene Pillay (2015) on using big data to prevent cyber fraud in South African banks revealed that South African banks have implemented big data analytics to combat cyber fraud. The study further mentions that banks in South Africa are eager to learn more about big data analytics and recommends that banks devote more time and effort to exploring and researching big data analytics capabilities (Pillay, 2015).

2.6 CONCLUSION OF LITERATURE REVIEW

2.6.1 Theoretical frameworks

The literature review on legislation and regulations revealed that digital fraud is regulated under cybercrime which is prohibited under the ECTA and the Common Law in South Africa. Research further revealed that South Africa introduced a cybercrime bill that will be implemented, but researchers argue that it will be ineffective for South African financial institutions, including banks and insurance companies. The ineffectiveness of the cyber bill is due to the fact that the bill does not include measures of AI, 5G and other technological measures. A study on digital fraud and safety tips suggested that identity theft risk can be moderated by implementation of rigorous policies.

Using technology was proven to be more effective in preventing digital fraud for financial institutions in South Africa. The study of technology in digital fraud revealed that the same ICT technology used by South African banks and insurance companies is also used by fraudsters when defrauding customers.

Education and awareness were proven to be effective ways to prevent fraud. The study suggested that customers should take responsibility for learning about the SABRIC website's information, as the website provides the latest information of digital fraud.

2.6.2 Conceptual frameworks

The conceptual framework for digital fraud knowledge management is connected to the study but does not form part of the overall digital fraud strategy plan, as other components which are very critical to the study including technology, governance and organisational structure are not included in the framework. Adopting the right tools or systems on digital platforms is critical and this conceptual framework does not take that into account. However, driving awareness through information sharing is important, amongst other elements for banks and insurance companies to combat digital fraud.

The conceptual framework for digital fraud risk management in banking provides a useful tool for banks and insurance companies to use to prevent digital fraud. Three elements are included in the model: the environment, the victim, and the fraudster. The study also suggests that it could be used in future financial or banking research involving participant surveys and interviews, which is relevant for this study as it incorporates both banks and insurance companies. The literature review on big data analytics revealed that such analytics is a good capability that can be used to build analytical models to predict, detect, respond to, and prevent fraud across the customer life cycle on digital platforms.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 RESEARCH METHOD

To analyse and understand the data for this research study, a quantitative and qualitative data method (mixed methods) will be used to analyse all issues discussed in the research study. Quantitative data approaches involve a systematic, standardised approach that includes surveys and asking questions (Muhammad & Kabir, 2016). The qualitative research method helps in the comprehension of more complex factors (Scalcău, 2021). A mixed-methods research is an approach in which statistical data extracted from quantitative data is supported and strengthened by qualitative data generated from the insights presented by research participants (Manzoor, 2020).

To answer the research questions, the mixed-methods approach was chosen because it allows for triangulation of findings (Scalcău, 2021). In a research study, triangulation is defined as the technique of integrating theories, methodologies or observations so that any biases resulting from using a single approach are eliminated (Noble & Heale, 2019). Triangulation enriches and allows data validation and can be applied to both quantitative and qualitative studies (Noble & Heale, 2019). The use of triangulation will help to clearly explain the findings of the research questions. The same results or findings from two different methods will increase confidence in the research findings.

3.2 RESEARCH DESIGN

Quantitative data is numerical and can be mathematically analysed. Quantitative data uses different scales, including nominal, ordinal, interval, and ratio scales (Muhammad & Kabir, 2016). An online survey will be conducted with a selected target audience in this study. Concurrent with the quantitative data, qualitative interviews will also be conducted. A qualitative study is designed to better understand the study's meanings and perspectives, with the primary goal of understanding rather than generalising across findings (Maxwell, 2012). According

to Epp and Otnes (2021), qualitative research identifies important problems, and drives the exploration of innovative, implementable, and strategic solutions.

Qualitative research will aid in gaining a better understanding of a practical digital fraud strategy framework for South African banks and insurance companies.

3.3 RESEARCH APPROACH

A mixed-method approach is used to address the research problem, broaden and deepen the conclusions of this study, and thus contribute to the existing literature. A mixed-methods approach aims to ensure validity, integration, interpretation, and correspondence by triangulating findings from quantitative and qualitative methods combined (Schoonenboom & Johnson, 2017).

The quantitative and qualitative data will be used to answer the study's questions, which are as follows:

- (1) What is a practical digital fraud strategy framework for banks and insurance companies in South Africa?
- (2) What factors impact digital fraud in banks and insurance companies in South Africa?
- (3) What impact does digital fraud legislation and regulations have on South African banks and insurance companies?

3.4 UNIT OF STUDY

The entity being studied in a research study is referred to as the unit of analysis, the determination of which is critical in any research project (Dolma, 2010). This study is about a digital fraud strategy framework for South African banks and insurance companies; thus, banks and insurance companies are the unit of study.

3.5 POPULATION

The population group for the research study are banks and insurance companies in the financial industry in South Africa. There are 36 national and international

banks licensed to operate in South Africa (Banking Association South Africa, 2021), 58 non-life insurance companies in South Africa (The South African Insurance Association, 2021), and 75 registered life insurance companies in South Africa (Financial Sector Conduct Authority, 2021). Therefore, the population group for this research study is made up of 169 financial companies within the banking and insurance sector.

3.6 SAMPLE SIZE

The sample size is an important aspect of a research study because it allows researchers to draw conclusions about a population based on a sample (Taherdoost, 2017). The unit of investigations were banks and insurance companies in South Africa. Nine banks and five insurance companies took part in the survey. The sample size for the research study was set at a minimum of 50 participants from banks and insurance companies at the executive head level to the middle-level management. A total of 67 responses from banks and insurance companies were recorded for the online survey. A sample of 15 participants was initially targeted to conduct structured interviews digitally. However, the researcher decided to conduct interviews with subject matter experts only to provide reliable, comparable data. Therefore, four subject matter experts were interviewed. The interviews were scheduled using video calls, and they were conducted using Microsoft Teams Meetings. The interviews were recorded and transcribed for analysis.

3.7 DATA COLLECTION PROCESS

Data that has never been collected before is known as primary data (Murphy, 2016). Primary data is more reliable and objective because it has never been collected or published previously. Primary data has a greater validity than secondary data that has previously been used (Muhammad & Kabir, 2016). Therefore, primary data will be used for this study.

The primary source of data used for this study is an online survey and structured interviews. Data from the online survey was collected and analysed using an SPSS statistical tool, and data from the interviews was analysed to obtain a better understanding of the research problem. Methods of analysis used include descriptive and inferential statistics (Regression analysis).

3.7.1 Ethics

According to Pan (2020), all research studies involving individuals must be approved by a duly authorised research ethics committee and the quality of a research study depends on the accuracy and ethical reporting of findings. An ethics clearance certificate was obtained from the University of the Witwatersrand Ethics Committee that is responsible for ensuring that policies or ethical conduct governing academic research are in place and also followed by researchers (refer to Appendix 2). Therefore, this study has been approved by the University of the Witwatersrand Ethics Committee and participants were guaranteed anonymity and confidentiality.

3.7.2 Informed consent

Participants' informed consent and voluntary participation is part of ethical conduct, which is required for research and to ensure participants that ethical requirements are met (Josephson & Smale, 2020). Participants were invited to participate in an anonymous online survey, and other participants were invited to participate in anonymous structured interviews. Formal participant consent information was included on the invites to all participants working in the banking and insurance sector (refer to Appendix 4 and 5 for the formal participant consent information for both the online survey and interviews, respectively). Participants were required to specify that they work for banks or for an insurance company before they could proceed with the survey or interview.

3.8 ANONYMITY AND CONFIDENTIALITY

The identities of participants will not be identifiable and disclosed throughout the research process. Restricted information such as participant names, company

names, company strategy and any other restricted information that could lead to the company information being identifiable was not requested to protect the identities of all participants as well as to protect the identities of the banks and insurance companies. Participants were informed that the information provided will be confidential and that they will not be identifiable or disclosed when responding to the survey questions or in the final report, and that their identities will not be disclosed. Participants were also informed that the data obtained from the study will not be made available to anybody else. Participants were informed about anonymity and confidentiality through the participant consent information and through the interview informed consent forms. The data obtained for the study will be protected and will not be shared with other individuals. The data will be saved in a laptop and both the laptop, and the data folder saved on the laptop will be password protected, and participants were also informed about this in the consent information.

3.9 VALIDITY AND RELIABILITY

Validity and reliability are significant elements in obtaining meaningful outcomes from research data (Rahi, 2017). Data extracted from the online survey will be validated through SPSS and the validation process will include computing and analysing outliers and missing data if found amongst other key aspects.

CHAPTER FOUR: PRESENTATION OF THE RESULTS

This research study combines mixed methods, namely quantitative and qualitative datasets, to conduct the data analysis. The first analysis will be carried out using SPSS data analysis software and the quantitative dataset will be collected through questionnaires. The qualitative data collected through interviews will be used in the second analysis, which will be conducted using ATLAS.ti data analysis software. To answer the research questions, both quantitative and qualitative analysis techniques will be used. The use of both quantitative and qualitative techniques is intended to improve the quality of the research findings. Section 4.1 will focus on quantitative data analysis, while Section 4.2 will focus on qualitative data analysis.

4.1 QUANTITATIVE DATA ANALYSIS

4.1.1 Descriptive quantitative dataset

The quality of the research analysis is based on the dataset used. It is important to have diverse observations from different people as this will bring variations to the data analysis, thus strengthening the research analysis and hence the findings. This section will describe the dataset collected. The aim is to show the diversity in the respondents.

The questionnaires were used to collect a total of 67 observations for the research. Of the 67 observations, 23 were dropped due to blank or unanswered questions. The questionnaires were specifically sent to participants who work in banks or insurance companies, and a screening question (Question number 1) was included in the questionnaires. Therefore, when the respondents answered no to the screening question, the survey ended, ultimately resulting in blanks or unanswered questions in the dataset. Of the 23 blanks or unanswered questions, 14 responded with a no to working in banks or insurance companies. In their respective institutions, 40.91 percent of the observations hold executive positions, while 59.09 percent are non-executive (Figure 6).

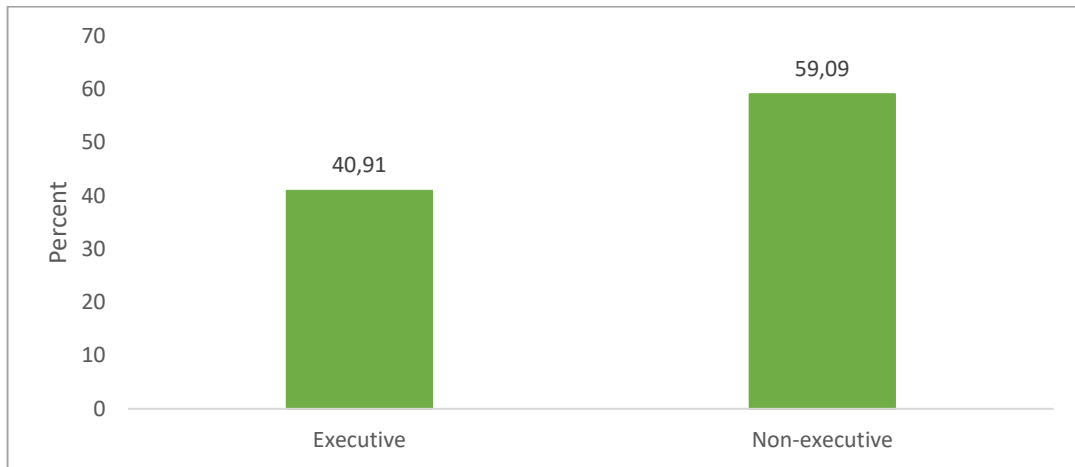


Figure 6: Position levels held by respondents
Source: (Data survey)

All the respondents are either from banking institutions or insurance institutions. A total of 77.27 percent of the respondents are from a banking institution and 22.73 percent are from insurance firms (Figure 7).

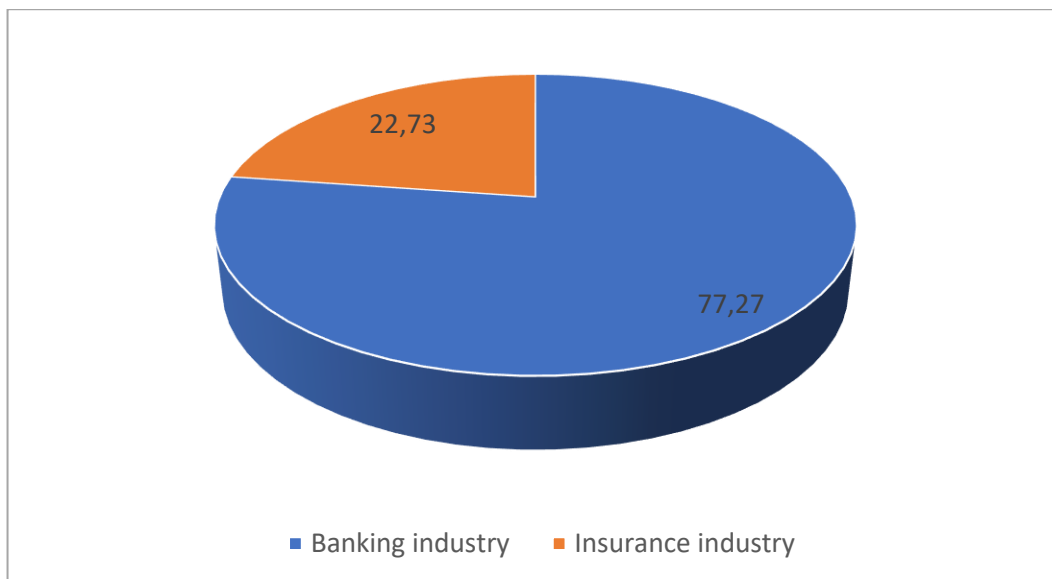


Figure 7: Banking and insurance composition
Source: (Data survey)

A further breakdown of the respondents shown in Table 1 depicts that the majority (50 percent) are executive heads of business units, 29.55 percent are middle managers and 9.09 percent are C-level executives, which include chief executive officers, chief operating officers and chief information officers (Table 1). The high-

level representation also points to the high quality of the responses and data collected.

Table 1: Percentage share of the position set of the respondents

Position	Percentage share
C-Level Executive	9.09
Executive Head of Business Unit	50
Middle Manager	29.55
Other	11.36

Source: Data survey

To further show the variations in the respondents, Figure 8 below displays the various departments and skills sets of the respondents. The skills sets are grouped into 13 groups, with the majority belonging to the digital group (18.18 percent), followed by strategy and innovation, data and analysis, legal, risk and compliance, each with a share of 13.64 percent. The least represented skills set groups are production management, actuarial and acquisition, each with a 2.27 percentage share representation.

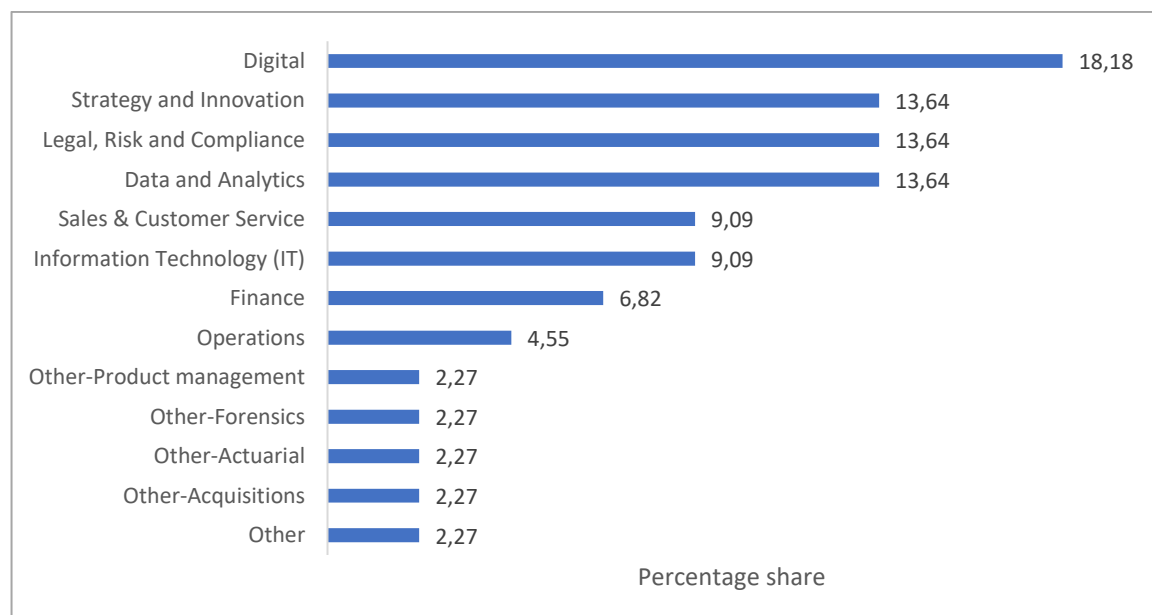


Figure 8: Skills set variations of the respondents

Source: Data survey

Based on the descriptive data analysis presented above, it can be observed that the sample size is good. The survey was successful in gathering information from

the targeted institutions as well as from the right personnel within those institutions. The respondents' diverse skills set, and position set demonstrate a great range of respondents, which should strengthen the research findings.

4.1.2 Evaluate a digital fraud strategy framework for banks and insurance companies in South Africa.

This section aims to evaluate a practical digital fraud strategy for banks and insurance companies in South Africa. Currently, different strategies are being used by different institutions captured in the questionnaire. The output of the different strategies in the form of the amount lost by the various institution through digital fraud per annum is included. The questionnaire also collects the revenue percentage lost by the institution as a result of digital fraud. The idea is that if an organisation has a good digital fraud strategy, it should therefore lose less revenue through digital fraud. The study aims to run a regression estimation with the strategy output being the dependent variable and the different strategy measures being the independent variables. In other words, the study seeks to establish the relationship between the digital strategy measures and the digital fraud output, which is the amount of money organisations lose through digital fraud.

Questions 11 and 24 from the questionnaire asked the respondents about the losses they incur through digital fraud. Questions 6–10 and 12–23 asked about the digital strategy measures that are in place in the respective institutions. The regression equation will be specified as:

$$Out = X'B + \varepsilon \dots\dots\dots 1.1$$

Where:

- *Out* is the digital fraud *output*, that is, the money lost by the institutions through digital fraud,

- X is a group of covariates representing the digital fraud strategy framework for the respective institutions (see Table 2), and
- ε is the idiosyncratic error term representing the uncollected factors that influence digital fraud in the respective institutions.

Two regression estimations will be done. The first model will have the questions individually represented as the independent variables. The second model will group the questions and construct an index which represents each respective group. Questions 6–8 will be grouped as Organisational structure variables, questions 9–10 as Legislation and regulation variables, 12–14 as Strategy variables, 15–16 as Technology variables, question 17 as Investigations variables, questions 18–21 as Education and Awareness variables, and questions 22–23 as Data and analytics variables.

Table 2: Variables' description

Variable	Variable Name	Variable description	Question number
Dependent variables			
<i>Out1</i>	Digital fraud amount	Annual digital fraud amount loss by organisations in Rands.	Q24
<i>Out2</i>	Digital fraud percentage	Annual digital fraud amount loss by organisations in percentage.	Q11
Independent/covariates			
<i>X1</i>	Responsible and accountable executive	An executive responsible and accountable for digital fraud in an organisation.	Q6
<i>X2</i>	Roles and responsibilities	Clearly defined roles and responsibilities of the digital fraud team in an organisation.	Q7
<i>X3</i>	Cross-functional working group	A cross-functional working group for digital fraud in an organisation.	Q8
<i>X4</i>	Policies	Policies applicable to organisations. Includes ethics policy, risk policy, digital or cyber fraud policy, fraud prevention policy and whistle-blowing risk policy.	Q9
<i>X5</i>	Legislation and regulations	Government legislation and regulations impact in combating digital fraud in organisations.	Q10
<i>X6</i>	Digital fraud strategy document	A written digital fraud strategy document in an organisation.	Q12

X7	Digital fraud risk assessments	Digital fraud risk assessments conducted in organisations.	Q13
X8	Risk-tolerance limit	A risk-tolerance limit regarding digital fraud in an organisation.	Q14
X9	Systems	Processes and systems in place for digital platforms in an organisation: <i>Device Intelligence</i> : To help customers in verifying identity, assessing and mitigating risk in real time, and improving customer experience. <i>Behavioural Biometrics</i> : To prevent identity-related digital fraud without disrupting users. <i>Personal Identifiable Information (PII)</i> : To identify customers by using information that, when used alone or in conjunction with other relevant data, can identify an individual. <i>In-App messaging</i> : To interact with digital platform users. <i>One-time pin</i> : To authenticate or provide security for digital transactions.	Q15
X10	Artificial Intelligence (AI)	Usage of AI technology for digital fraud (for example, biometrics, face recognition).	Q16
X11	Forensics	A forensic or investigations department that proactively drives investigations for digital fraud in an organisation.	Q17
X12	Digital fraud campaign	Digital fraud awareness and educational campaigns that organisations drive.	Q18
X13	Latest digital fraud information (modus operandi)	Latest information on new digital fraud scams shared by an organisation to prevent fraud.	Q19
X14	Fraud awareness training	Ongoing digital fraud awareness training offered by organisations.	Q20
X15	Employee awareness	Employee awareness on the organisation's position regarding digital fraud.	Q21
X16	Big data	Use of big data for digital fraud by organisation in order to prevent, predict, detect, monitor, respond and evaluate.	Q22
X17	Analytical models (Predictive and preventative)	Use of predictive and preventative models by organisation to prevent and predict digital fraud.	Q23

Source: Data survey

4.1.3 Data coding

The responses from the questions in Table 2 were coded, thus converting the string variables to numeric. The coding was done by assigning numerical numbers to the respective responses as follows: strongly disagree is assigned a numerical value of 1, disagree = 2, somewhat disagree = 3, neither agree nor disagree = 4, somewhat agree = 5, agree = 6, and strongly agree = 7.

The summary statistics of the coded responses are depicted in Table 3.

Table 3: Summary statistics

Variable	Observations	Mean	Standard deviation	Minimum	Maximum
Ungrouped statistics (Individual questions)					
Q6	44	5.977	1.285	2	7
Q7	44	5.681	1.474	2	7
Q8	44	5.409	1.661	2	7
Q9	44	4.659	1.964	1	11
Q10	44	5.522	1.067	2	7
Q11	44	10.909	11.527	0	50
Q12	44	4.977	1.6773	1	7
Q13_31	44	67.909	27.122	9	100
Q14	44	5.227	1.538	1	7
Q15	44	4.409	1.041	1	5
Q16	44	5.181	1.781	1	7
Q17	44	4.772	2.390	1	7
Q18	44	75.022	28.508	8	100
Q19	44	5.545	1.634	2	7
Q20	44	5.772	1.428	2	7
Q21	44	5.522	1.284	2	7
Q22a	40	67.375	28.618	9	100
Q22b	42	55.095	28.533	0	100
Q22c	40	69.95	26.698	3	100
Q22d	43	65.674	28.845	0	100
Q22e	40	68.4	31.566	2	100
Q22f	38	64.736	30.341	2	100
Q23	42	5.142	1.539	2	7
Q24	24	6725000	4287298	500000	1.00e+07
Grouped statistics (Group questions)					
Organisation	44	17.068	3.842	8	21
Strategy	44	78.113	29.106	14	114
Technology_1	44	4.409	1.041	1	5
Technology_2	44	5.181	1.781	1	7
Investigation	44	4.772	2.390	1	7
Legislation_1	44	4.659	1.964	1	11
Legislation_2	44	5.522	1.067	2	7
Awareness	44	91.863	30.870	19	121
Analytics	36	397.972	160.400	72	607

Source: Data survey

Questions 11, 13, 18, 22 a-f and 24 were already in numerical terms, thus there was no need for coding. Question 9 asked the respondents to select the policies that apply to their organisation, and thus cannot be coded as the other questions explained above. Thus, the coding here should allow a comparison of the different policies used in the various organisations. For question 9, the coding will be as follows:

Code Number	Code Name
1-	for Ethics policy only
2-	for Risk policy only
3-	for Digital or cyber fraud policy only
4-	for Fraud policy, Ethics policy, Risk policy, Digital or cyber fraud policy, Fraud prevention policy, Whistle-blowing risk policy only
5-	for Fraud policy, Ethics policy, Risk policy, Fraud prevention policy, Whistle-blowing risk policy only
6-	for Whistle-blowing risk policy only
7-	for Ethics policy, Risk policy, Fraud prevention policy, Whistle-blowing risk policy only
8-	for Fraud policy, Ethics policy, Risk policy, Digital or cyber fraud policy only
9-	for Risk policy, Digital or cyber fraud policy, Fraud prevention policy only
10-	for Fraud prevention policy only and
11-	for Fraud policy, Risk policy, Digital or cyber fraud policy, Fraud prevention policy, Whistle-blowing risk policy only

The response to question 15 (Technology in place on digital platforms) will compare the technology or process and systems provided with Device Intelligence. Thus, question 15 is coded as Device Intelligence and assigned a numerical value of -5, Behavioural Biometrics will be assigned a value of -4, Personal Identifiable Information -3, In-App messaging -2 and One-time pin will be assigned a value of -1. In the regression estimation, one technology or process and system will be dropped, and the remaining technologies or processes and systems will be compared to the technology dropped. The summary statistics table displays the observations, mean, standard deviations, and minimum and maximum values of each variable. The number of observations should be 44 for all variables, however, questions Q22a–Q22e and Q23 have missing responses. A standard deviation is a

measure of how dispersed the data is in relation to the mean. Low standard deviation means that the data is clustered around the mean, and high standard deviation indicates data that it is spread out. The standard deviation shows more spread-out variables for Q24 and Q22a–Q22f (Data & Analytics and Education & Awareness) as they have relatively higher standard deviation (Table 3). This is a positive outcome, as more variation will improve the regression estimation.

4.1.4 Diagnostic test statistics

Before running the regression equation 1.1, a correlation matrix was created. A correlation matrix is a table which displays the correlation coefficients among the variables. It is best used in variables that demonstrate a linear relationship between each other. Variables with a correlation coefficient greater than 0.8 should not be included in the same regression, thereby creating multicollinearity (Shrestha, 2020). Multicollinearity is a statistical concept that describes the correlation of several independent variables in a model (Young, 2017). The correlation matrix in Appendix 7 shows that Q22a, Q22b–Q22f, Q17 and Q13 have high correlation coefficients. As a result, the regression estimation will exclude variables with correlation coefficients greater than 0.8.

4.1.5 Regression estimations

Aligned with the abovementioned diagnostic test, dataset and model, the researcher estimated the regression equation model in Equation 1.1. Table 4 displays the regression estimates from Model 1. With a significant F-statistic of 0.007, an R-squared of 0.6218, and an adjusted R-squared of 0.5268, the regression is a good fit. The F-statistics test is a global test that determines whether or not all predictor variables jointly explain the dependent variable. If the p-value of the F-statistic is less than 0.05, the conclusion can be reached that all explanatory variables are statistically significant in explaining the dependent variable (Keith, 2015). The R-squared or the Adjusted R-squared is a statistical measure that

represents the proportion of a dependent variable's variation that independent variables can explain in a regression model.

An R-squared value of $0.3 < r < 0.5$ is generally considered weak, while an R-squared value of $0.5 < r < 0.7$ is generally considered as having a moderate effect size. A strong effect size is defined by an R-squared value of $r > 0.7$ (Knoke, Bohrnstedt, & Mee, 2002). The regression estimated below produced a strong R-squared statistic of 0.6218.

The remaining regression estimates are shown in Table 4 below. Column one contains the dependent variables, column two contains the regression estimation, and column three contains the p-values which will be used to determine the significance of the estimated regression coefficient. A p-value of less than <0.05 indicates that the estimated regression coefficient is significant at the 5 percent level. The revenue percentage lost by organisations due to digital fraud is the dependent variable in the estimation. Thus, a negative and statistically significant coefficient means that the digital fraud strategy measure greatly reduces the revenue share lost due to digital fraud. Digital fraud measures with such characteristics must therefore be recommended to the organisations, as statistically they significantly reduce revenue lost due to digital fraud.

Table 4 demonstrates that only seven digital fraud strategy measures statistically and significantly reduce the share of revenue lost due to digital fraud, namely: Q6, Q7, Q9_5, Q9_6, Q18, Q19, Q22f and Q23. This means having an executive who is accountable and responsible for digital fraud (Q6), having clearly defined roles and responsibilities for one's digital fraud team (Q7), having a Fraud policy, Ethics policy, Risk policy, Fraud prevention policy and Whistle-blowing risk policy only (Q9_5), having a Whistle-blowing risk policy only (Q9_6), having strong digital fraud awareness and educational campaigns (Q18), sharing the latest information on new digital fraud scams to prevent fraud (Q19), use of big data for digital fraud (Q22f),

and use of predictive and preventative models to prevent and predict digital fraud (Q23) statistically and significantly reduce the share of revenue lost due to digital fraud. Thus, the above measures are the most effective digital fraud strategy framework for banks and insurance institutions in South Africa. Such organisations which have the above strategy measures strongly in place have been observed to lose relatively less revenue through digital fraud.

4.1.6 Robustness checking

The questions are then categorised into groups as organisational structure variables, legislation and regulation variables, strategy variables, technology variables, investigation variables, education and awareness variables, and data and analytics variables. As there are two legislation and regulation variables (Q9 – Legislation-1 and Q10 – Legislation-2) and two technology variables (Q15 – Technology 1 and Q16 – Technology 2) which are coded in a way that makes combining them difficult, two more models will be run separately to account for each of the un-combinable variables. The regression estimates for the two additional models are displayed in Table 5 and 6.

Table 4: SPSS regression coefficients estimation model-1

Variables	Regression coefficient	P-value
Q6	-1.014	0.044
Q7	-9.587	0.023
Q8	-3.657	0.242
Q9_4	-2.413	0.101
Q9_5	-2.478	0.049
Q9_6	-3.202	0.048
Q9_7	2.770	0.142
Q9_8	-9.092	0.084
Q9_9	-5.552	0.090
Q9_10	-6.900	0.055
Q10	-1.486	0.064
Q12	-7.394	0.128
Q14	-7.062	0.124

Q15_2	-2.430	0.267
Q15_3	-5.707	0.076
Q15_4	2.333	0.179
Q15_5	6.543	0.487
Q16	-1.418	0.088
Q17	-2.021	0.133
Q18	-0.684	0.031
Q19	-6.726	0.044
Q20	7.379	0.194
Q21	-1.065	0.067
Q22c	-0.903	0.068
Q22d	-0.550	0.074
Q22f	-1.459	0.030
Q23	-7.313	0.031
_cons	-5.548	0.021

Source: SPSS regression table using the survey coded dataset. The dependent variable is the revenue percentage lost by the institutions through digital fraud, F-statistic is 0.007, R-squared of 0.6218 and an adjusted R-squared of 0.5268.

Table 5 shows that organisational variables, Legislation (5 – Fraud policy, Ethics policy, Risk policy, Fraud prevention policy, Whistle-blowing risk policy only) and 6 (Whistle-blowing risk policy only), as well as Awareness and Analytics, statistically and significantly reduce the share of revenue lost due to digital fraud (Table 5).

The model fitness is also robust with a significant F-test statistic of 0.000, and a high R-squared of 0.559.

Table 5: SPSS regression coefficients estimation model-2

Variables	Regression coefficient	P-value
Organisational	-0.018	0.019
Strategy	-0.152	0.451
Technology_1-2	7.054	0.756
Technology_1-3	-6.343	0.076
Technology_1-4	-4.308	0.783
Technology_1-5	-3.142	0.829
Investigations	-0.465	0.686
Legislation_1-4	-6.599	0.710
Legislation_1-5	-2.021	0.013
Legislation_1-6	1.493	0.032
Legislation_1-7	-2.508	0.159
Legislation_1-8	-4.503	0.052
Legislation_1-9	-7.253	0.068
Legislation_1-10	1.693	0.413

Legislation_1-11	-1.828	0.227
Awareness	-0.233	0.027
Analytics	-0.002	0.034
_cons	-1.751	0.026

Source: SPSS regression table using the survey coded dataset. The dependent variable is revenue percentage lost by the institutions through digital fraud, F-statistic is 0.000, R-squared of 0.559 and an adjusted R-squared of 0.536.

Using the alternative variables of Technology, that is, Technology_2 and an alternative Legislation variable, that is, Legislation_2, Table 6 shows that only organisational variables, awareness, and analytics can statistically and significantly reduce the share of revenue lost due to digital fraud. The model fitness is also strong with a significant F-test statistic and high R-squared¹.

Table 6: SPSS regression coefficients estimation model-3²

Variables	Regression coefficient	P-value
Organisational	-0.077	0.022
Strategy	-0.074	0.627
Technology_2	-1.733	0.349
Investigations	-0.793	0.458
Legislation_2	-1.844	0.403
Awareness	-0.008	0.006
Analytics_1	-0.004	0.046
_cons	-19.067	0.023

Source: SPSS regression table using the survey coded dataset. The dependent variable is revenue percentage lost by the institutions through digital fraud, F-statistic is 0.002, R-squared of 0.489 and an adjusted R-squared of 0.4468.

4.1.7 Conclusion on quantitative analysis

This section aimed to conduct the quantitative analysis. Firstly, descriptive statistics were used to analyse the questionnaire responses, and discovered a good sample size and a significant variation in the responses. Secondly, organisational variables, selected legislation variables, awareness and analytics variables were found to be the statistically significant variables in reducing revenue lost due to digital fraud. As

¹ F-statistic is 0.002, R-squared of 0.489 and an adjusted R-squared of 0.4468

² Using alternative variables for Technology and Legislation

a result, organisations in the banking and insurance sector should aim to have the abovementioned measures in place to reduce digital fraud.

However, organisations should aim for specific measures under the broad or grouped variables: Organisational variables, Legislation, Awareness and Analytics. Under Organisational variables, organisations should aim to have a strong executive who is responsible and accountable for digital fraud (Q6) and have strong clearly defined roles and responsibilities of their digital fraud team (Q7).

Under Legislation, banking and insurance organisations should strive on having the right policies in place, namely: Fraud policy, Ethics policy, Risk policy, Fraud prevention policy and Whistle-blowing risk policy (Q9_5 and Q9_6). Organisations should aim for strong digital fraud awareness and educational campaigns (Q18), as well as sharing the most recent information on new digital fraud scams to prevent fraud (Q19). Under Data and Analytics, institutions should strive to use big data for digital fraud (Q22f) and predictive and preventative models to prevent and predict digital fraud (Q23).

4.2 QUALITATIVE DATA ANALYSIS

In addition to the data collected through the questionnaires, four interviews were conducted. The study's aim was to collect qualitative data that validates or reviews additional information on the quantitative statistics provided in the questionnaires. The participants interviewed are subject matter experts working in digital fraud or fraud departments at various banks and insurance companies. The interview questions are grouped into different categories, namely, demographics, organisational structure, legislation and regulations, strategy, technology, investigations, education and awareness, and data and analytics. The analysis will also be organised following the groupings of questions. A qualitative analysis software, ATLAS.ti was used to explore the various responses of the participants interviewed. ATLAS.ti is a qualitative research computer program. Researchers and

practitioners use the software package in various fields such as economics, educational sciences, engineering, management studies, market research and quality management, among others. This study will use various tree diagrams to connect the various points of view and responses under each question grouping.

4.2.1 Descriptive qualitative dataset

Figure 9 shows the distribution of the respondents' duties and roles in their various institutions starting with demographics. The skills set of the participants interviewed determines the strength of the response. Figure 9 clearly shows that the appropriate participants were interviewed, as they are all involved in digital fraud roles in their respective workplaces.

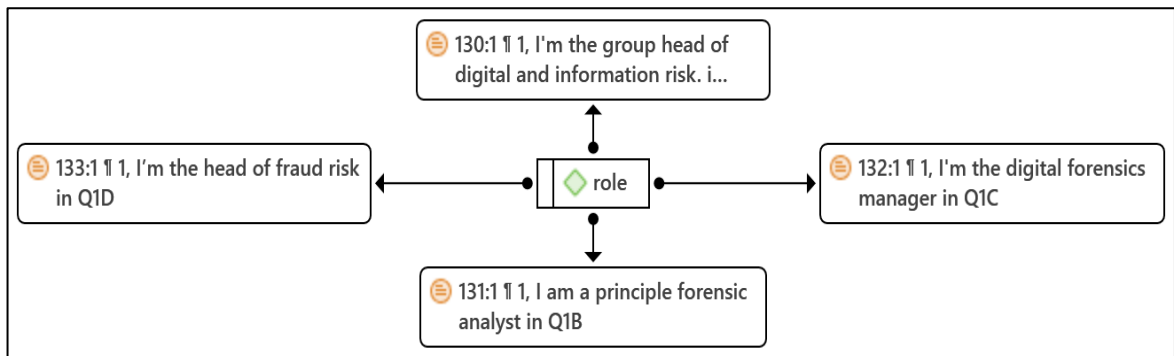


Figure 9: Distribution of roles and duties of the participants' interviewed
Source: ATLAS.ti output using the interviews dataset

Figure 10 shows a summary of the activities performed in the departments of the respondents. The functions listed include digital portfolio management, managing the external digital framework, and risk management in internet banking, among others.

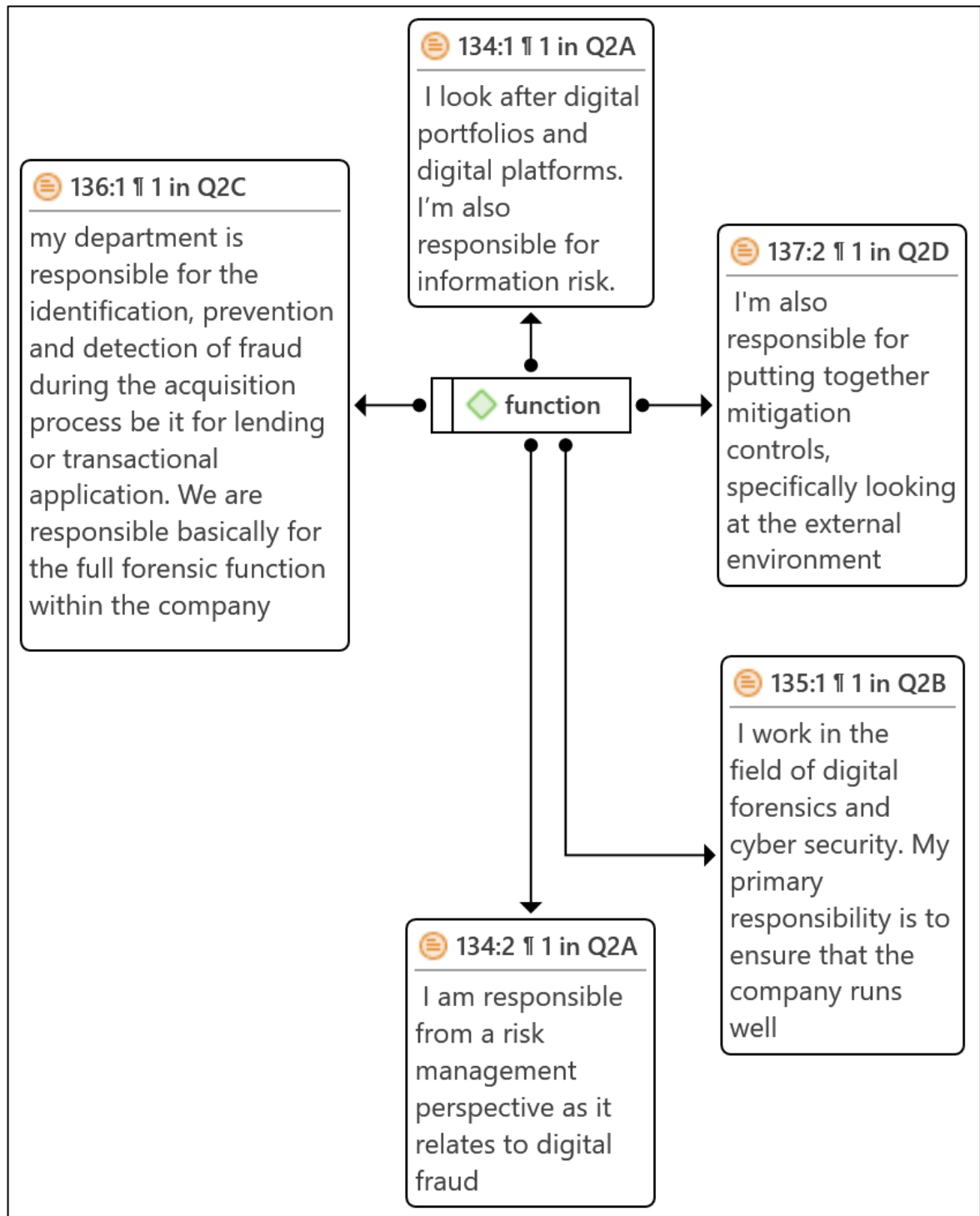


Figure 10: Department functions of the interview participants
Source: ATLAS.ti output using the interviews dataset

4.2.2 Organisational structure

Two questions were asked, one about clear roles and responsibilities and the other about cross-functional working groups for digital fraud management. All participants

in this study cited a well-defined and organised digital fraud department with clear roles and responsibilities. The participants described the connection of all stakeholders in the fraud value chain, including fraud risk management teams, IT security teams, forensic teams, and security and operations teams. There is consensus among the participants on the importance of clearly defining roles in digital fraud departments (this is depicted in Figure 11). The concept of a robust cross-functional group was strongly recommended (this is illustrated in Appendix 8). Cross-functional cooperation is required, as digital fraud typically affects multiple product streams. For example, in the banking industry, there are numerous platforms such as cloud platforms and vendor engagement platforms. These various platforms have multiple sub-platforms and products. As a result, there is a great need for a cross-functional team, as there cannot be a single digital fraud team for each of these multiple products and platforms.

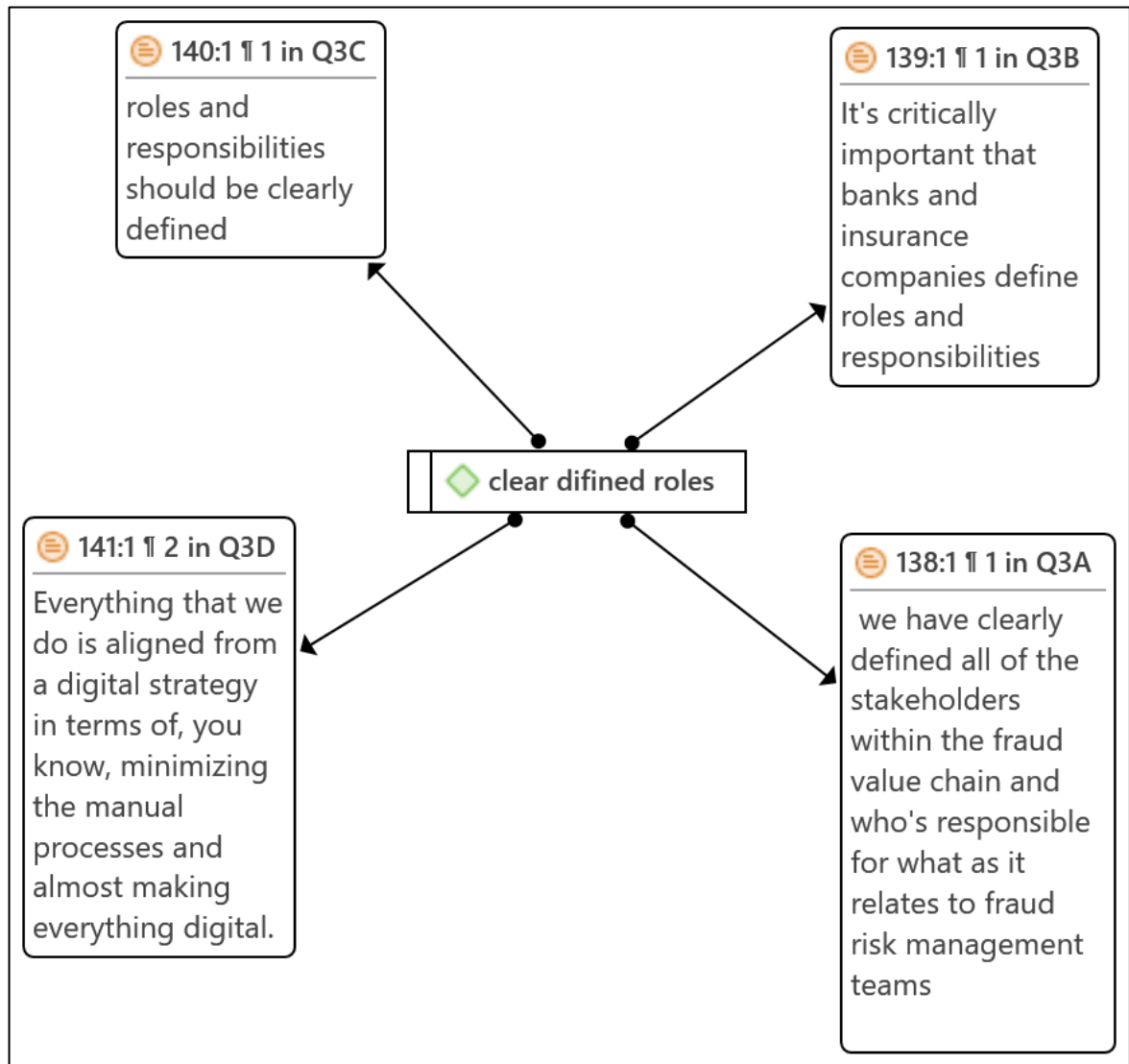


Figure 11: Defined roles and responsibilities
Source: ATLAS.ti output using the interviews dataset

4.2.3 Legislation and regulations

Questions were asked regarding group fraud policy documents, ethical policy documents, fraud prevention policy, cyber or digital fraud policy, and whether or not staff members understood these policies. The participants confirmed that they had the various documents in their various institutions. However, some participants explained that they name the documents differently and that some are incorporated into one document. Some policy documents exist, but they are not specific to digital fraud. Staff members' perceptions of whether the policy documents are well understood are generally mixed. Some institutions have plans to use training better to communicate the policies to upper and lower employees.

Some of the responses mentioned using an induction training programme to communicate the policy to new employees. The induction programme assists staff in understanding the policy; however, some components covered in the induction training are general and not specific to the digital fraud department, implying that continuous training programmes are always required. The summary of responses to cyber digital policy documents are shown in Figure 12 below. The tree diagrams of the responses on fraud policy documents, ethical policy documents, and fraud prevention policies are shown in appendices 9–11.

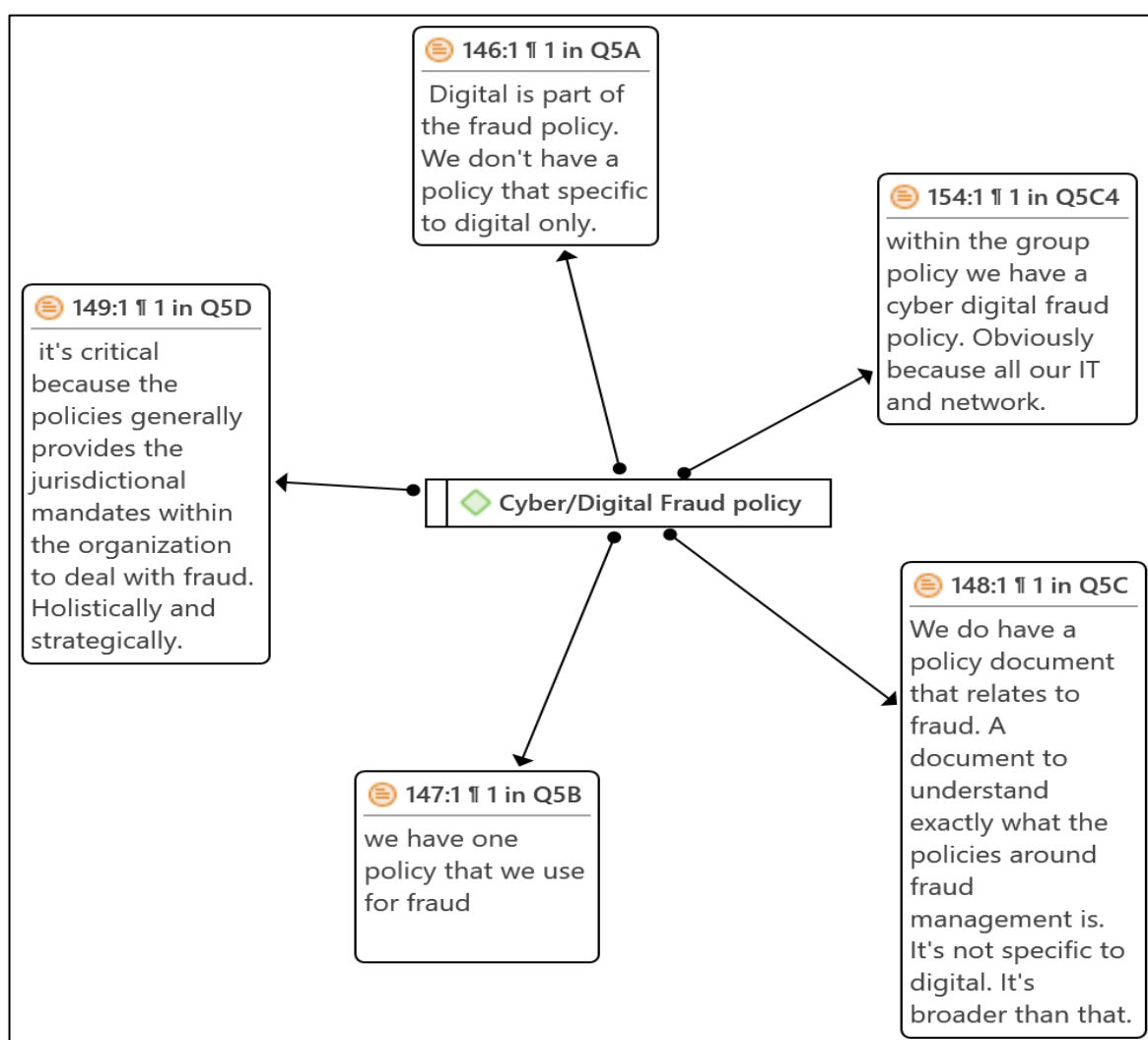


Figure 12: Summary of responses on cyber digital policy documents
Source: ATLAS.ti output using the interviews dataset

In terms of the impact of government policy on internal fraud policies, respondents expressed that government policy had a relatively minor impact on their internal digital fraud policies. Most participants mentioned that internal fraud mitigation

plans play a more critical role than government fraud mitigation plans. The government provides little to no assistance to banks and insurance companies regarding fraud prevention and awareness. No internal policy should override legal requirements, hence fraud policies must be highly aligned with government regulations and legislation, such as the Banks Act, Insurance Act, Electronic Communications and Transactions Act, Personal Information Protection Act, and Cyber Crime Act, among others.

4.2.4 Strategy

The respondents expressed concern about the percentage of the company's earnings loss attributed to digital fraud. A point was made that there should be no acceptable percentage loss, and that any loss is unacceptable. Participants all stated that most organisations experience a zero to five percent revenue loss due to digital fraud. This is mainly attributable to the stronger controls they have put in place to reduce the risk of digital fraud. The responses to the share of revenue loss due to digital fraud are summarised in Figure 13 below.

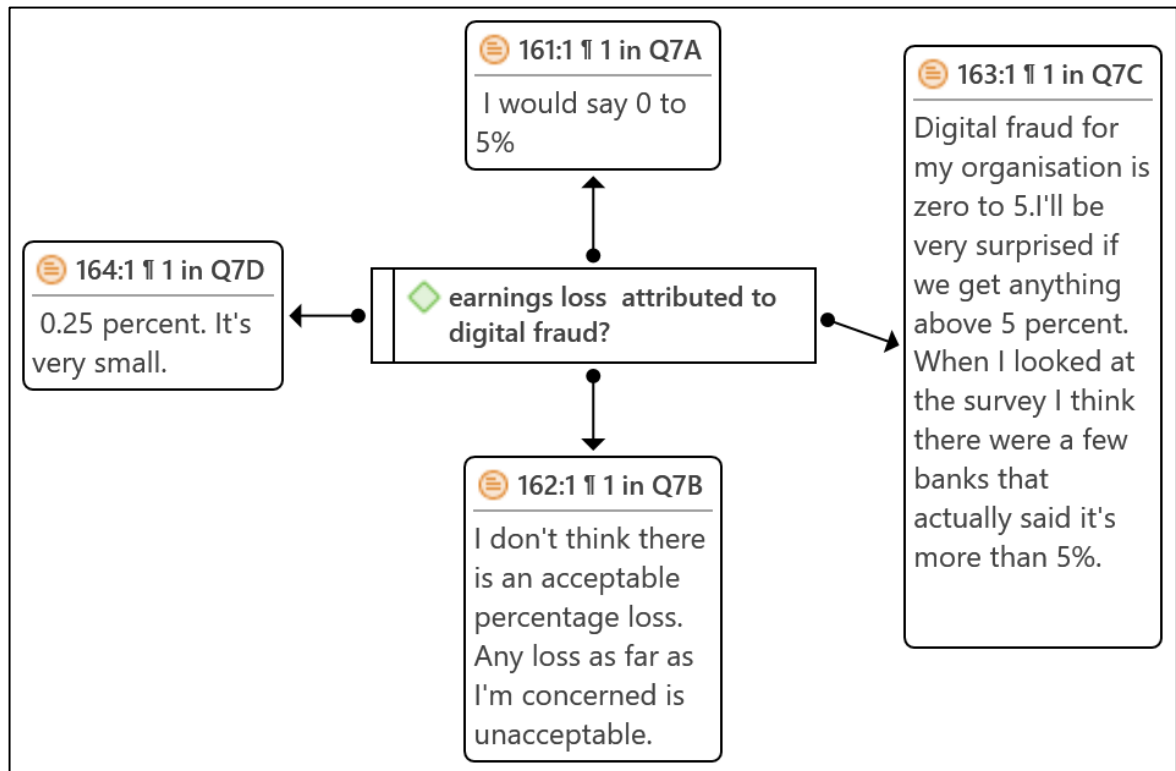


Figure 13: Percentage of earning losses due to digital fraud
Source: ATLAS.ti output using the interviews dataset

4.2.5 Technology

Participants were asked about the presence of various security processes and systems, such as Device Intelligence, which assists customers in verifying identity, assessing and mitigating risk in real time, and improving customer experience, behavioural biometrics that assists customers with preventing identity-related digital fraud without interfering with user experience, Personal Identifiable Information (PII) that identifies customers, in-app messaging that is used to interact with mobile application users, one-time pin or password that is used for each transaction made, and Artificial Intelligence (AI) which includes technologies such as biometrics and facial recognition. Figure 14 shows the responses to the question of AI. Appendix tables 12–15 show responses on Device Intelligence, Behavioural Biometrics, In-App Messaging, and Personal Identifiable Information. There were some definition differences among the interview participants, but the general consensus was that all of the above platforms were present in all of the organisations.

The use of the technologies however varies from organisation to organisation. Some organisations have more sophisticated technologies than others, but there are plans to upgrade to better systems. In terms of device identification, the responses indicated that security varies depending on the device being used by the customer, as some devices require multiple authentications. However, the organisations have a security technology that registers frequently used devices when transacting.

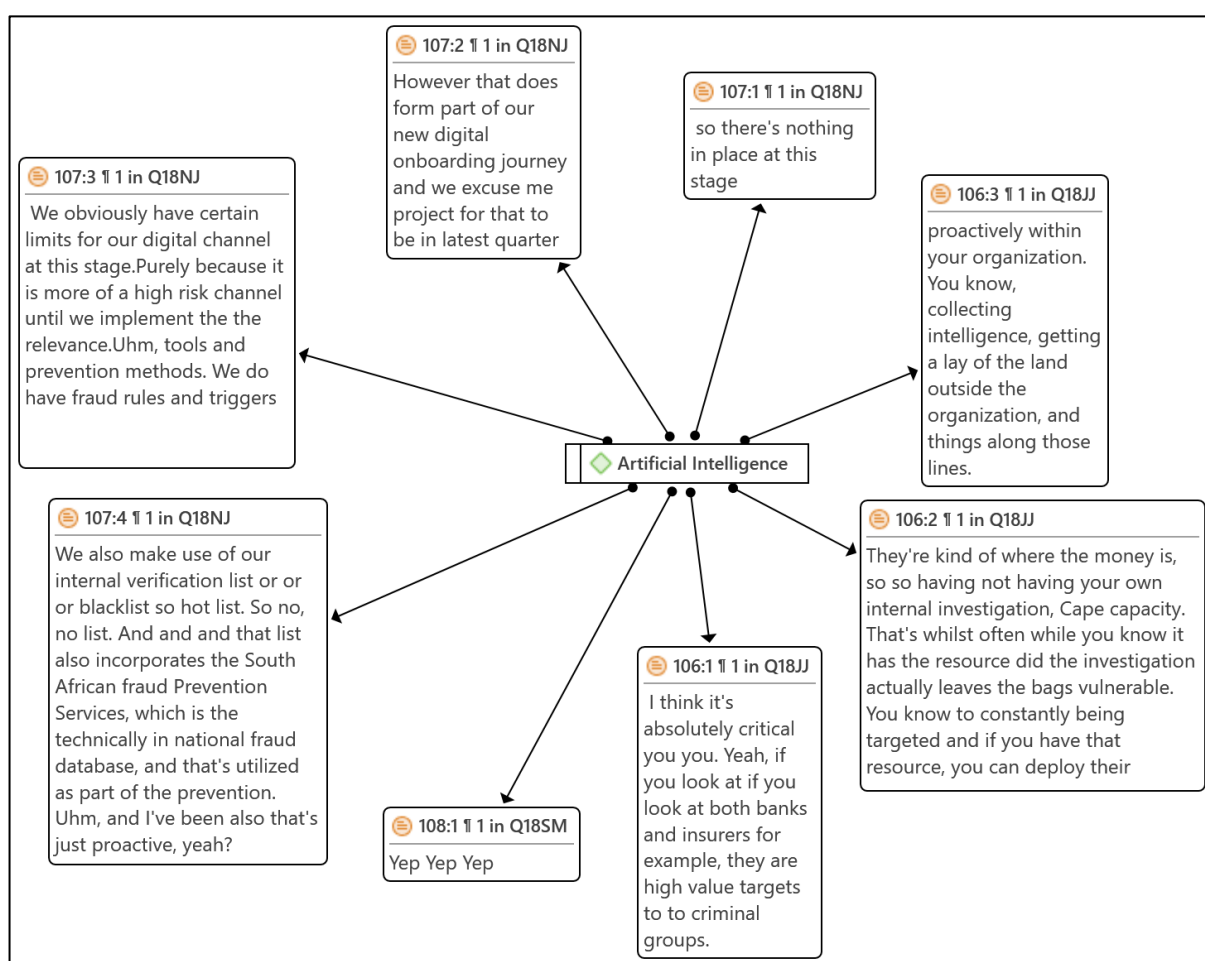


Figure 14: Responses regarding the use of AI
Source: ATLAS.ti output using the interviews dataset

The use of a new device will then require additional authentication. Some customer identification issues are mandated by the national credit regulator, Financial Intelligence Centre Act (FICA), and Anti-Money Laundering (AML). The responses also mentioned a high level of coordination with the Department of Home Affairs, primarily for the verification of customer information. It was also mentioned that the

level of security and authentication varied depending on the type of transaction. Transactions involving large sums of money require additional authentication compared to transactions involving small amounts of money.

4.2.6 Forensics

The respondents were asked about the presence of forensic or investigations departments that proactively drive investigations for digital fraud. A further question in this section asked if the organisation conducts proactive digital fraud investigations. Figure 15 shows the responses on forensic investigation departments.

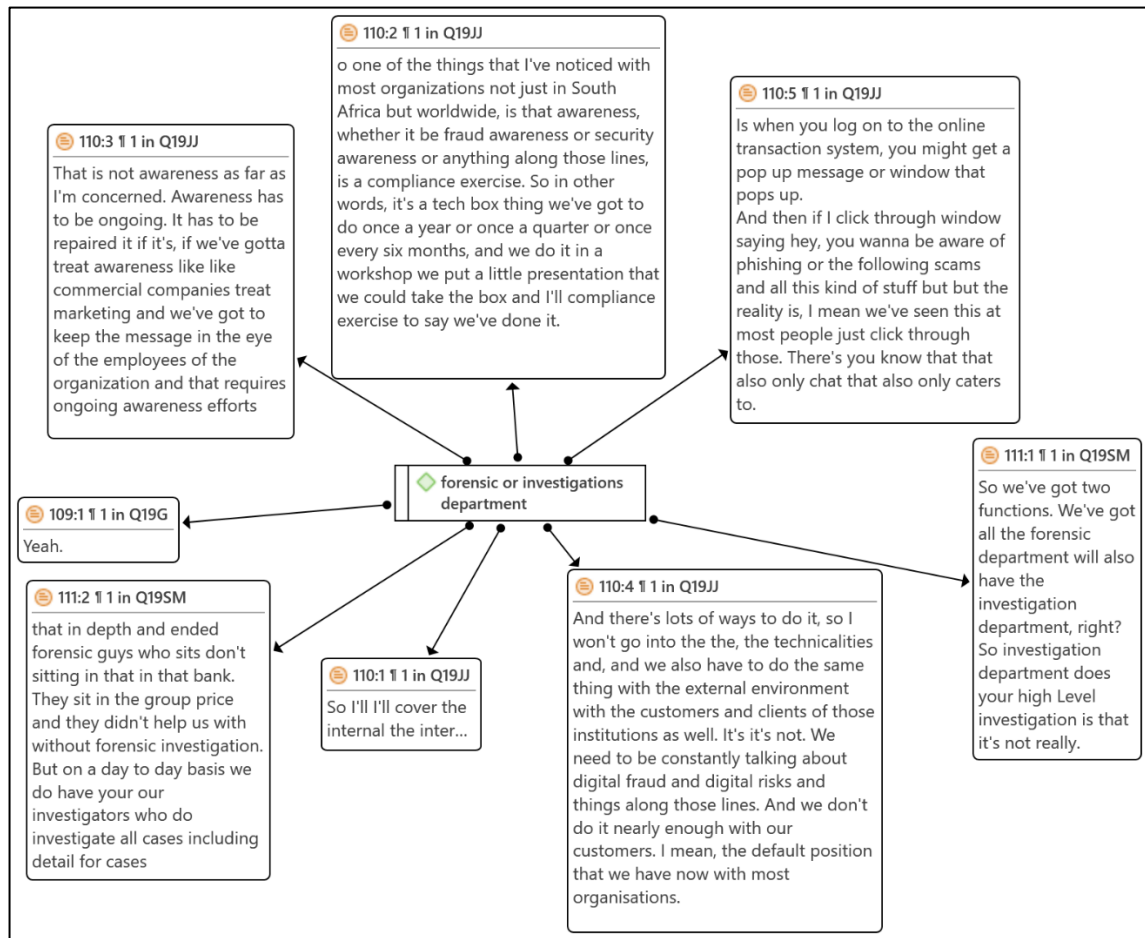


Figure 15: Responses on forensic or investigation department
Source: ATLAS.ti output using the interviews dataset

All participants acknowledged the presence of a forensic or investigation department, as well as proactive investigations for digital fraud. The departments are described as highly organised. The quality of the investigation, however, varies across organisations.

4.2.7 Education and awareness

A question was posed about how organisations drive digital fraud awareness and educational campaigns both internally and externally. There was also a question about how organisations share the latest information on new digital fraud scams used by fraudsters on digital platforms.

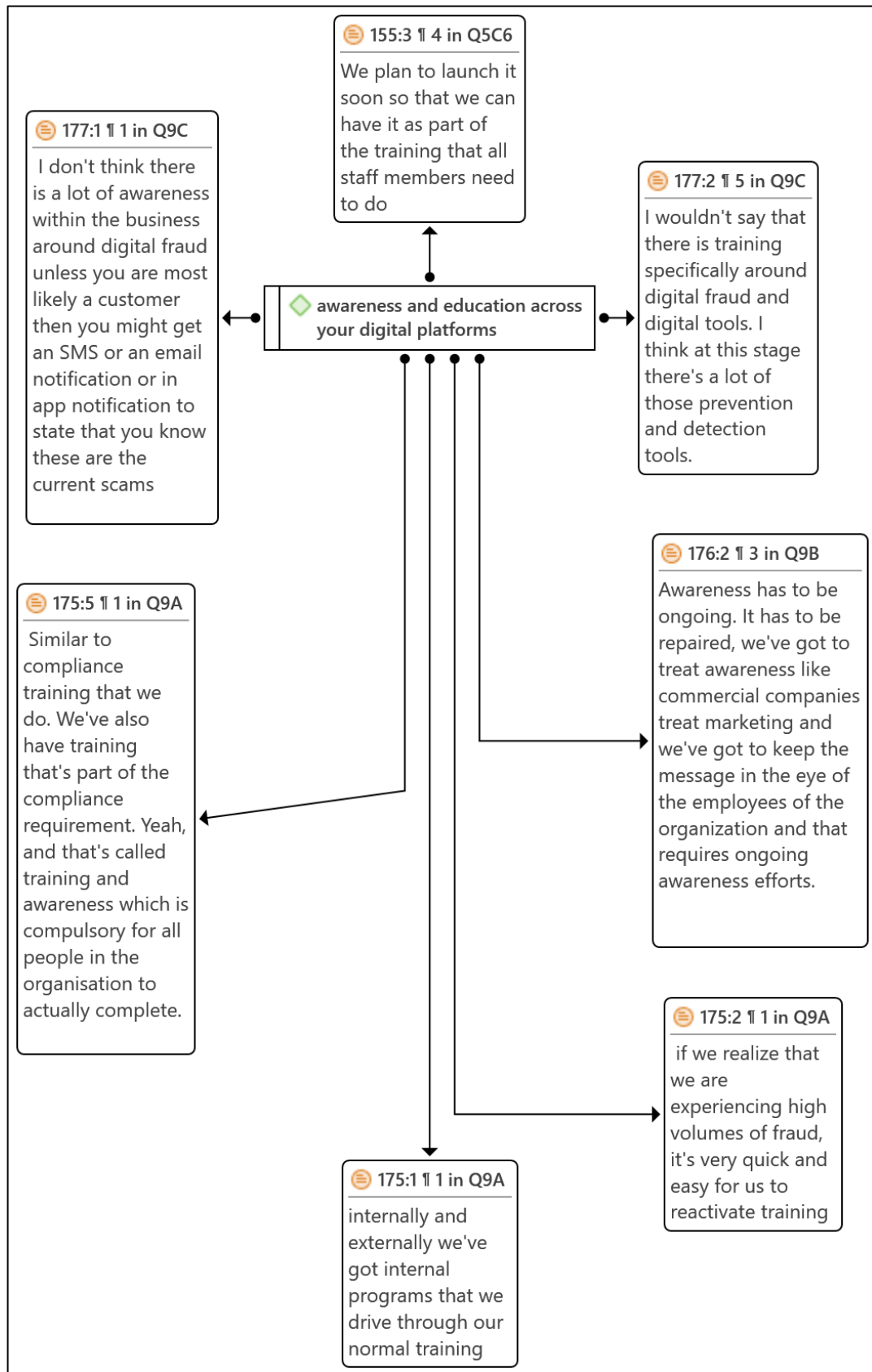


Figure 16: Education and awareness campaigns, external
Source: ATLAS.ti output using the interviews dataset

Some organisations expressed concern about driving internal and external awareness campaigns, while others explained that they drive these effectively. Despite the fact that staff in digital fraud departments are more aware of fraud, a need to constantly upgrade the skills of the staff through effective methods of sharing new fraud techniques and through the adoption of better devices and systems was also raised. Ongoing training for digital fraud staff was raised as a concern. Collaboration across departments, across organisations, and international corroboration were raised as requirements for reducing digital fraud among banks and insurance companies. The need for ongoing communication with customers, as well as the sharing of tips on how to be cautious, were also mentioned as critical factors to consider. It was recommended that such campaigns be expanded through the use of other platforms such as social media, radio and television channels, rather than digital channels only.

4.2.8 Data and analytics

There were two questions about the use of big data to prevent digital fraud. The second question focused on analytical models for predicting and preventing digital fraud throughout the customer life cycle. Figure 17 depicts the responses to the use of big data. In general, the organisations acknowledged the use of big data in their operations in attempts to prevent fraud and in the development of models that predict and prevent fraud. Organisations are at various stages of utilising big data. The participants also agreed that greater use of big data should reduce digital fraud significantly. A decision for some banks and insurance companies to increase their investment in the use of big data to combat fraud has been made.

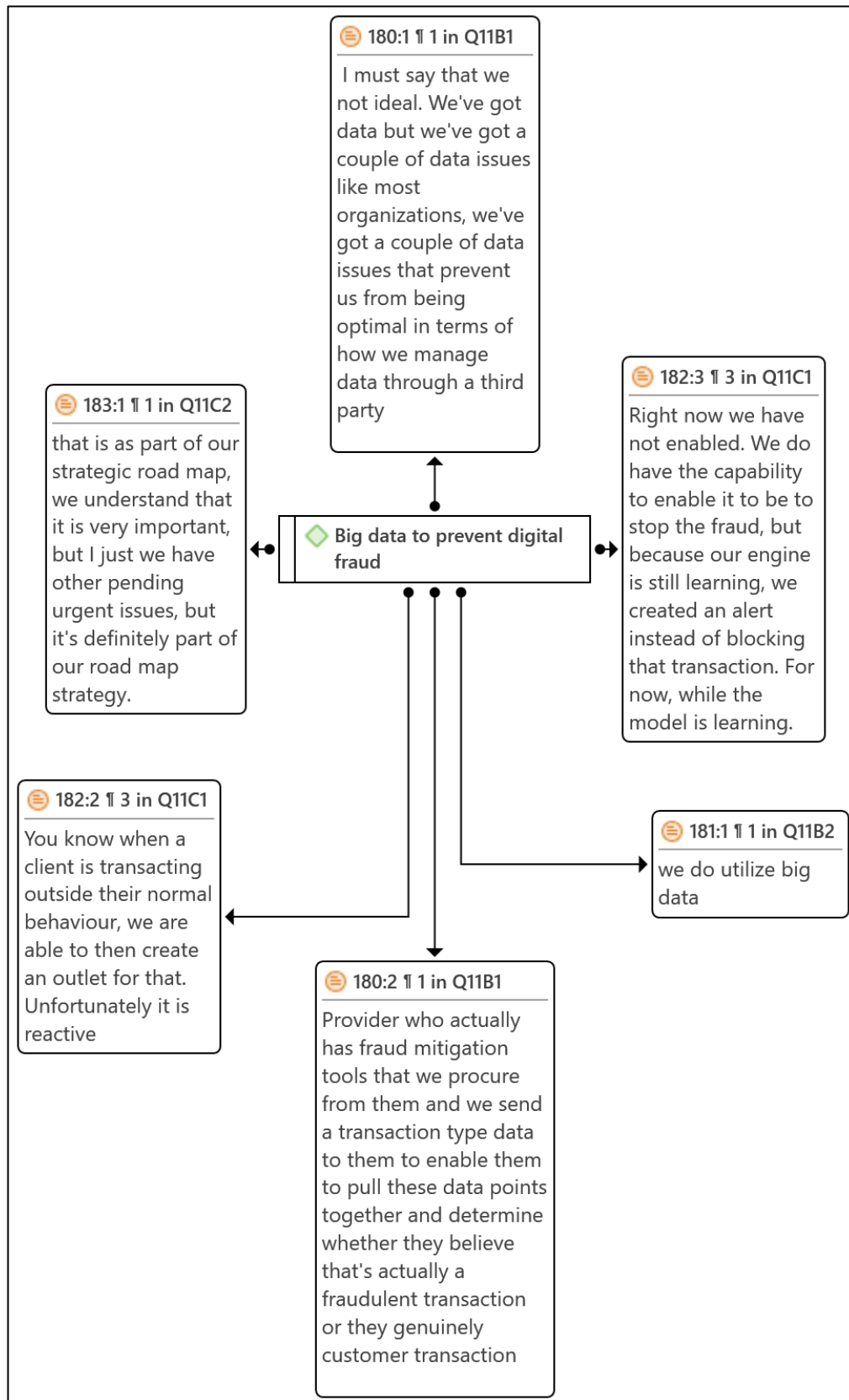


Figure 17: Big data to prevent digital fraud
Source: ATLAS.ti output using the interviews dataset

4.2.9 Conclusion on qualitative analysis

The aim of this section was to present the results of the qualitative analysis. Atlas.ti, a qualitative data analysis software, was used for the analysis. The qualitative analysis discovered additional issues that were not addressed by the quantitative analysis. Digital and fraud departments in banking and insurance organisations generally have robust organisational structures with clear roles and responsibilities and a high degree of cross-functional working groups across different business units and products. The majority of banking and insurance companies have internal policy documents such as a fraud policy, ethics policy, fraud prevention policy, and a cyber/digital fraud policy. These policies are very much in line with government regulations and legislation. However, more help might be needed from the government towards mitigating digital fraud. It was also discovered that banks and insurance companies have technologies that help in mitigating fraud, such as Device Intelligence, behavioural biometrics, personal identification information, in-app messaging, and one-time pins. A strong recommendation was made to raise fraud awareness among both employees and customers. Banks and insurance companies should invest in big data and the development of analytical models that predict and prevent digital fraud.

CHAPTER FIVE: DISCUSSION OF THE RESULTS

5.1 Introduction

The main aim of this study was to evaluate a digital fraud strategy framework for South African banks and insurance companies using quantitative and qualitative analysis. The results presented in Chapter Four will be discussed in this chapter and integrated with the literature review discussed in Chapter Two.

For quantitative analysis, two regression models were completed, with one model representing questions individually and the other model representing individual questions as respective groups. For qualitative analysis, four subject matter experts were interviewed in order to obtain additional insights that the quantitative analysis did not provide.

5.2 Legislation and regulations

Based on the literature review discussed in Chapter Two, digital fraud is regulated under cybercrimes in South Africa, which are prohibited under the Electronic Communications and Transactions Act (ECTA), Common Law and the National Cybersecurity Policy Framework, but the study argues that these laws have not been effective in combating digital fraud (Chitimira & Ncube, 2021). The study by Chitimira and Ncube on the cybercrime bill that is yet to be enacted further argued that the cybercrime bill will not effectively combat digital fraud because the bill does not include measures of technology such as Artificial Intelligence (AI) and fifth-generation network technology for financial companies.

This study evaluated policies and the impact of government legislation and regulations on digital fraud in South African banks and insurance companies. The quantitative analysis of this study found that having the right policies in place can statistically and significantly reduce the share of revenue lost due to digital fraud. The policies assessed included the fraud policy, ethics policy, risk policy, fraud prevention policy, and whistle-blowing risk policy. The qualitative analysis also found that policies and measures that the banks and insurance companies have

implemented have an impact on digital fraud. In some institutions, the study found that there is one fraud policy which incorporates other policies such as digital or cyber fraud. The qualitative study further revealed that employee training and onboarding processes are used to ensure that employees understand these policies, and that the policies should be easy to understand and constantly reviewed.

Having the right fraud policies in place, and the tools to support them, can assist banks and insurance companies to reduce digital fraud losses. While both qualitative and quantitative analysis revealed that the right policies impact reducing digital fraud loss for banks and insurance industries, government legislation and regulations had no impact on combating digital fraud, as the quantitative results for legislation and regulations were statistically insignificant in both regression models. The qualitative results also supported the finding, as most banks and insurance companies specified that financial organisations have no support from the government with regard to digital fraud prevention.

In terms of legislation, the qualitative results described clients as being more protected from digital fraud than banks and insurance companies, as they have organisations such as the Ombudsman. The latter proactively drive investigations on their behalf and mostly favour clients. This means that the measures and controls that the banks and insurance companies have put in place such as constant review of fraud policies, ongoing training with employees and embedding fraud policies as part of the onboarding processes, have greater impact in reducing digital fraud loss for banks and insurance companies as compared to government legislation and regulations.

5.3 Education and awareness

A study conducted in 2015 revealed that education and awareness are the most effective ways to reduce cyber fraud in banking (Dzomira, 2015). The South African Banking Risk Information Centre (SABRIC) has also stated the important role of education and awareness in preventing digital fraud. The literature review also

argued that customers need to use the information made available on the SABRIC website to be well informed on new fraud scams. Most banks in South Africa are members of SABRIC, and they utilise the information or insights that SABRIC provides to combat digital fraud. SABRIC encourages customers to stay well informed on new modus operandi in the financial industry and they also encourage banks to communicate with their customers on new fraud scams. The South African Fraud Prevention Service (SAFPS) is another organisation that is focused on preventing fraud in banks and insurance companies in South Africa.

Having strong digital fraud awareness and educational campaigns or initiatives, and sharing the latest information on new digital fraud scams to prevent fraud have proven to be statistically significant in the study. The qualitative results indicated that education and awareness are effective and form part of the compliance exercise that employees must complete in banks and insurance companies. Some respondents indicated that banks and insurance companies treat education and awareness initiatives as a tick-box that must be completed at a specified period of time and that awareness has to be ongoing. Some respondents indicated the need to find more dynamic ways for people to engage with the content on digital platforms to help them obtain a better understanding about digital fraud. In line with this, one of the participants suggested: *“a better option would be, for example, before you transact – here's a short, 32-second video that you have to watch, instead of a pop-up window that says you have to click yes to proceed with a transaction”*.

Interviewees mentioned that campaigns should be expanded through the use of other platforms such as social media, radio, and television channels, and that instead of focusing on driving digital fraud campaigns on digital platforms, banks and insurance companies should focus on effectively communicating with customers.

It was also noted that banks and insurance companies should find ways for customers to interact with their digital fraud content, rather than alerting customers about fraud when they see that a customer is about to complete an activity on their digital platforms.

5.4 Organisational structure

Three questions were asked under organisational structure based on the first regression model, which ran the questions individually. The first question asked whether having an executive accountable for digital fraud in an organisation has an impact reducing digital fraud (Q6). The second question was to ascertain whether clearly defined roles and responsibilities for digital fraud teams having has an impact on reducing digital fraud (Q7). The final question under organisational structure asked if having a cross-functional team helps to reduce digital fraud (Q8). Q6 and Q7 statistically demonstrated that having an executive accountable and responsible for digital fraud and having clearly defined roles and responsibilities for the digital fraud team significantly reduce the share of revenue lost due to digital fraud. On the second regression model, the three questions were categorised into one organisational group. The results revealed that organisational structure statistically and significantly reduced the share of revenue lost due to digital fraud. Interview participants agreed on the importance of clearly defining roles for a digital fraud team and the concept of a robust cross-functional working group was strongly supported.

5.5 Technology

This study assessed whether organisations have tools to help them prevent digital fraud from a security perspective. Participants were asked to choose the tools that were applicable to their organisations (Q15). The tools included Device Intelligence, which aids in identity verification, risk assessment and mitigation in real time, and customer experience improvement. Other tools mentioned included behavioural biometrics to prevent identity-related digital fraud while minimising user disruption, in-app messaging used to interact with users by pushing digital fraud scams that customers should be aware of, Personal Identifiable Information used to aid in identifying of customers by utilising information that, when used alone or in conjunction with other relevant data, can identify an individual, and end-to-end encryption used to secure communication platforms by preventing unauthorised

users from accessing transferred data. Another question was about AI technology (Q16), which includes the use of biometrics and face recognition for identification.

Both Q15 and Q16 were found not to be statistically significant in reducing digital fraud in both regression models. However, the interviews revealed some definition differences in how the participants interpreted the concepts of the tools in Q15. The general consensus was that all of the technology tools mentioned in Q15 were present in most organisations. Regarding Q16, some organisations mentioned that they have a biometric capability but as an opt-in capability and that their adoption rates for it are low. Most of the organisations mentioned that they do have in-app messaging but also highlighted that they do not have in-app authentication. One of the participants discussed the difference between in-app messaging and in-app authentication. In-app messaging was defined as a function on the mobile app that allows the organisations to send educational or awareness messages. By authentication, organisations are moving away from one-time password authentication via SMS or email and towards in-app authentication messaging because the two channels can be intercepted. Therefore, authentication is integrated into the app. About three banks were mentioned to have in-app authentication in South Africa. Device Intelligence was mentioned as one of the tools that is helping organisations to register or identify customers using their mobile device data. Almost all organisations mentioned that they use one-time pins on their digital platforms. However, they also highlighted that one-time pin are ineffective unless they are incorporated with other tools such as a device identifier. Despite the technological tools being statistically insignificant in the regression models, the interviews revealed that most organisations have these tools in place to help combat digital fraud. A literature review also revealed that fraudsters target customers for digital fraud using the same technology as banks and insurance companies.

5.6 Big data and analytics

Big data and analytical models were evaluated, and the use of big data for digital fraud (Q22f), and the use of predictive and preventative models to predict and

prevent digital fraud (Q23), were found to be statistically significant in reducing the share of revenue lost due to digital fraud.

The qualitative analysis found that most organisations have data issues, as they do not have one central data and analytics environment. As a result, developing robust analytic models to predict and prevent fraud throughout the customer life cycle is challenging. All organisations agreed that big data is critical in the digital fraud space to help prevent and predict fraud in real time, and in predicting digital fraud. One bank manages data through a third party, which has mitigation tools that they procure from.

Previous research studies show that most banks and insurance companies have implemented big data, but the studies also highlight that most of the banks are still in the process of learning more about big data analytics.

To maximise fraud detection and prevention effectively, relevant datasets must be created, and the datasets must also be maintained and applied by banks and insurance companies. Predictive analytics capability that detects fraudulent activity as early as possible with minimal disruption to business decisions or the customer experience is critical for organisations.

5.7 Investigations

To gain a better understanding of investigations in banks and insurance companies, questions about investigations and/or the forensics function were asked to determine whether this business function aids in the reduction of digital fraud. The study found that this function does not statistically and significantly reduce the share of revenue lost due to digital fraud. The interviewees all agreed that they have forensics and/or investigations function. One bank mentioned that they have both a forensics department and an investigations department. The former does not form part of the banking structure but sits outside the bank, and the investigations' function deals with high-level investigations and does not conduct in-depth investigations.

5.8 Strategy

Banks and insurance companies should have a fraud risk strategy which clearly shows the needs of the business and is supported by a culture of fraud risk awareness and control across the entire organisation. The digital fraud output, which is the money lost by institutions as a result of digital fraud, was used as an output or dependent variable in this study, because if banks and insurance companies implement the right strategy plans, fraud losses will ultimately reduce. The output was measured using a set of covariates discussed in the literature review, and new variables were added to obtain a better understanding of an effective digital fraud strategy framework for banks and insurance companies.

The CIMA management risk cycle recognises important factors that organisations must implement in order to have an effective fraud strategy framework (CIMA, 2009). The first step highlighted in the risk management cycle is to establish a risk management group with the function of facilitating and coordinating the overall risk management cycle; it further highlights that the risk management group should form a committee that meets on a regular basis to discuss the set goals. The first step is identified outside the actual risk management cycle itself, implying that organisations must establish a group who will manage the business's overall fraud risks. Once a fraud risk management group has been established, the business's risk areas must be identified. The third step of the cycle is fully understanding and assessing the magnitude of the risk. The fourth step is creating a risk response strategy, the fifth step is to implement the strategy into action and assign responsibilities, the sixth step is implementing the suggested controls in place and monitoring them, and the final step entails refining the process and repeating it.

The strategy section evaluated if the organisations had strategy documents in place, and if banks and insurance companies conducted digital fraud risk assessments. Fraud risk assessments are fundamental factors that should be incorporated by banks and insurance companies as part of their overall strategy, as shown in the risk management cycle above, and the strategy for digital fraud needs to be very clear and well understood by everyone in the organisations.

The regression models revealed that strategy does not statistically and significantly reduce the share of revenue lost due to digital fraud. Despite the fact that both regression models in this study statistically showed that the strategy section does not impact digital fraud reduction, factors such as organisational structure, education and awareness, legislation, and other key factors are all incorporated in the strategy framework, all of which this study showed statistically and significantly have a huge impact in reducing the share of revenue lost as a result of digital fraud. Other studies discussed in Chapter Two have also shown that components of the strategy framework such as education and awareness have an impact in reducing digital fraud numbers. Key factors discussed in the above fraud risk management cycle were evaluated in this study and have shown to have an impact in digital fraud reduction, namely: organisational structure (roles and responsibilities), education and awareness (culture), legislation and regulations (governance), technology, and big data and analytics. The majority of interviewees indicated that their organisations suffer a zero to five percent revenue loss as a result of digital fraud. A critical point was raised in the interviews by South Africa's most qualified digital or cyber fraud expert when asked what, in their opinion, was an acceptable percentage loss in an organisation's earnings as a result of digital fraud. The interviewee stated the following: *"There should be no acceptable percentage loss due to digital, any loss due to digital fraud should be considered unacceptable"*.

After understanding the fraud triangle discussed in the literature review, it is critical for banks and insurance companies to understand that as their digital strategies evolve and organisations fail to implement controls or measures to mitigate their fraud risks, fraudsters are more likely to commit fraudulent activities as they evolve their fraudulent ways as well. It is clear from the results discussed above that having the right measures or controls in place is very critical in reducing digital fraud.

5.9 The digital fraud strategy framework

As discussed in Chapter One, the primary objective of this study is to evaluate a digital fraud strategy framework for South African banks and insurance companies.

Research studies revealed that there is currently no digital fraud strategy framework for banks and insurance companies that incorporates all of the key components of an effective digital fraud strategy. Studies also revealed that components of a holistic digital fraud strategy framework do not exist. This research study evaluated the following primary question in order to contribute to existing research studies and also provide a strategy framework that banks, and insurance companies can use to combat digital fraud in their organisations:

1. What is an effective digital fraud strategy framework for banks and insurance companies in South Africa?

The survey results found seven digital fraud measures that significantly reduce digital fraud, or the share of revenue lost to digital fraud for banks and insurance companies. The measures that were found to be effective are listed below and summarised in Table 18:

- Having an executive who is accountable and responsible for digital fraud
- Having clearly defined roles and responsibilities for the digital fraud team
- Having the right policies in place, including fraud policy, ethics policy, risk policy, fraud prevention policy and whistle-blowing risk policy
- Having strong digital fraud awareness and educational campaigns
- Sharing the latest information on new digital fraud scams to prevent fraud
- The use of big data for building predictive and preventative models to prevent and predict digital fraud

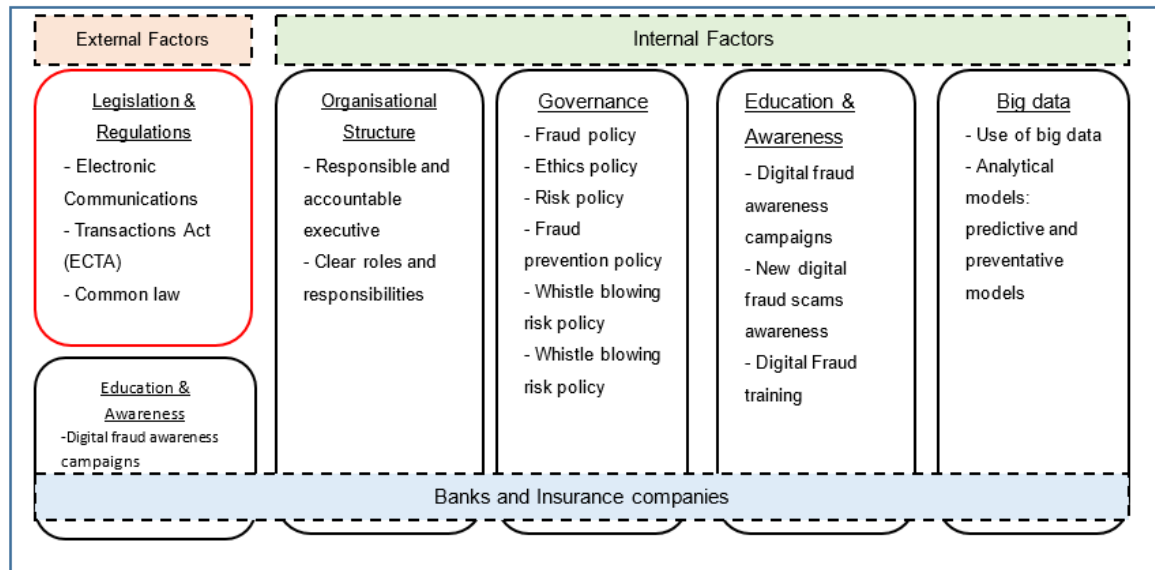


Figure 18: A digital fraud strategy framework for banks and insurance companies
Source: Survey and interviews results

The measures outlined above are the most effective digital fraud strategy measures for South African banks and insurance companies. Banks and insurance companies that have implemented the aforementioned strategy measures have been observed to lose less revenue due to digital fraud. Accordingly, the measures outlined above represent an effective digital fraud strategy framework for South African banks and insurance companies. The study found that the government legislation and regulations (external factors highlighted in red) do not have an impact on reducing digital fraud for banks and insurance companies in South Africa. However, from a governance perspective, the internal policies that have been implemented by the organisations have an impact on reducing the amount of digital fraud.

The secondary questions of this study were as follows:

1. What impact does digital fraud legislation and regulations have on South African banks and insurance companies?
2. What factors impact digital fraud in banks and insurance companies in South Africa?

Section 5.2, which discussed legislation and regulations, revealed that the right policies help to reduce digital fraud in South African banks and insurance companies. However, the research revealed that the measures put in place by banks and insurance companies to support their policies are more effective, while government measures were statistically found to be insignificant when it comes to reducing fraud for the organisations. The findings were supported by both the quantitative results and qualitative results, as the organisations specified that financial organisations have no support from the government as it relates to digital fraud prevention. One participant explained that banks and insurance clients are adequately protected by government legislation as they have organisations such as the Ombudsman which proactively drive investigations on their clients' behalf, provided the investigations fall within their jurisdiction. The participant further explained that banks and insurance companies are not adequately protected against syndicated digital or cyber fraud.

The study identified over 20 variables, which were then evaluated in order to fully understand the factors that impact digital fraud in South African banks and insurance companies. The seven factors listed above were discovered to have an impact on digital fraud, as discussed in the results section.

CHAPTER SIX: CONCLUSION

6.1 Introduction

The research findings presented in Chapter Four were discussed in the previous chapter of this study. To address the research problem of the increase in the amount of digital fraud in banks and insurance companies, existing literature was reviewed to better understand why the research problem persists. Existing literature revealed that one of the challenges that banks and insurance companies face is a lack of legislation. Other studies found that technology, education, and awareness can help banks and insurance companies combat digital fraud. This chapter will review the objectives of the research study and revisit the research questions posed in the first chapter to see if the research objectives were met and if the research questions were answered.

6.2 Research objectives

The primary objective of this research was to evaluate an effective digital fraud strategy framework for South African banks and insurance companies. This objective was achieved, and the digital fraud strategy framework for banks and insurance companies is provided in the previous chapter.

The primary research question of the study was answered in detail in Chapter Five: *What is an effective digital fraud strategy framework for banks and insurance companies in South Africa?*

The secondary objective was to assess the factors that have an impact on digital fraud. The regression models discussed in Chapter Four revealed the factors that have an impact on digital fraud, the results of which were also supported by the qualitative analysis conducted. This secondary objective was also achieved.

The secondary research question of the study was answered in detail in Chapter Five: *What factors impact digital fraud in banks and insurance companies in South Africa?*

The third objective was to evaluate the impact of digital fraud legislation and regulations for South African banks and insurance companies. This objective was also achieved, as the findings from the study revealed that government legislation and regulations have no impact on combating digital fraud. The research revealed that the internal policies that govern the digital fraud strategies for banks and insurance companies impact the digital fraud strategies for banks and insurance companies in South Africa.

The third research question of the study was answered in detail in Chapter Five: *What impact does digital fraud legislation and regulations have on South African banks and insurance companies?*

Existing research revealed that some components of a digital strategy for combating digital fraud existed; however, the research identified a gap, as a holistic digital fraud strategy framework did not exist. Therefore, this research has contributed to the existing research by bridging the gap. This was achieved by evaluating a strategy framework that comprises organisational structure, strategy, legislation and regulations, education and awareness, technology, big data and analytics, and investigations. A study conducted by Rachel Barker revealed that fraud prevention strategies and policies are needed in the South African financial sector (Barker, 2020).

6.3 Policy suggestions

Based on the results discussed in Chapter Four, government legislation does not have an impact in reducing digital fraud for banks and insurance companies in

South Africa. The study found that measures that the banking and insurance organisations have put in place are more effective compared to government legislation. The study revealed that embedding measures such as training to drive awareness with employees on their internal policies is more effective.

Tools that banks and insurance organisations implement to combat digital fraud need to be incorporated into legislation. Digital platforms differ from physical platforms. Banks and insurance companies need to improve their processes and systems when it comes to identity verification of customers. Current policies do not include essential measures that banks and insurance companies are beginning to incorporate into their processes, such as Artificial Intelligence (AI) and other important technological measures that could potentially expose the financial services industry to new fraud risks.

The study also revealed that while bank and insurance clients are protected by organisations such as the Ombudsmen, financial service providers are not. Policies should also consider the financial service providers for cyber fraud investigations, as cyber syndicate fraud is currently not considered in existing policies.

The cybercrime bill to be enacted should consider measures that should be implemented by financial service providers such as identity verification tools.

6.4 Suggestions for future research

The study found that government legislation does not impact digital fraud reduction and that organisations have the right measures in place to reduce fraud. Further research can be conducted to better understand government's legislation, with a focus on the new cybercrime bill to be enacted and the jurisdiction of policies.

This study focused on South African banks and insurance companies; a similar study could be conducted for Fintech companies.

Future research on AI technology to combat digital fraud may also be conducted. Fraudsters use customers' information to commit digital fraud, therefore integrating AI processes and systems with other verification systems, such as Home Affairs systems, to verify customers in real time can be evaluated.

REFERENCES

- Abdullahi, R., & Mansor, N. (2015). Fraud Triangle Theory and Fraud Diamond Theory. Understanding the Convergent and Divergent For Future Research. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, 1-8.
- Ahmed, M., Ansar, K., Muckley, C. B., Khan, A., Anjum, A., & Talha, M. (2021). A semantic rule based digital fraud detection. *Peer J Computer Science*, 1-21.
- Banking Association South Africa. (2021, October). <https://www.banking.org.za/about-us/member-banks/>. Retrieved from banking.org.za: <https://www.banking.org.za/about-us/member-banks/>
- Barker, R. (2020). The use of proactive communication through knowledge management to create awareness and educate clients on e-banking fraud prevention. *South African Journal of Business Management*, <https://doi.org/10.4102/sajbm.v51i1.1941>.
- Bernstein, J., Brits, M., Ketley, R., Mela, M., Mogadime, K., Naidoo, B., . . . Wapenaar, K. (2017). *The impact of the 4th industrial revolution on the South African financial services market*. Centre of Excellence in Financial Services.
- Bhasin, M. L. (2016). Integration of Technology to Combat Bank Frauds: Experience of a Developing Country. *Wulfenia*, 1-34.
- Cait, C. (2020). Conceptual and theoretical frameworks in research. *Research Starters*, 1.
- Chitimira, H., & Ncube, P. (2021). The Regulation and Use of Artificial Intelligence and 5G Technology to Combat Cybercrime and Financial Crime in South African Banks. *PER - DOI*, 1-33.
- CIMA. (2009). *Fraud Risk Management: A Guide to Good Practice (second edition)*. United Kingdom: Chartered Institute of Management Accountants.
- Dolma, S. (2010). The central role of the unit of analysis concept in research design. *Department of Organizational Behavior, School of Business Administration*, 1-6.
- Drew, J. M., & Farrella, L. (2018). Online victimization risk and self-protective strategies: developing police-led cyber fraud prevention programs. *POLICE PRACTICE AND RESEARCH*, 2-14.
- Dziak, M. (2020). Theoretical Framework. *Salem Press Encyclopedi*, 1.
- Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. *Risk Governance and Control Financial Markets & Institutions*, 1-13.
- Dzomira, S. (2015). "Cyber-banking fraud risk mitigation conceptual model". *"Banks and Bank Systems"*, 1-9.
- Dzomira, S. (2015). Cyber-banking fraud risk mitigation conceptual model. *"Banks and Bank Systems"*, 1-9.

- Dzomira, S. (2015). ONLINE & ELECTRONIC FRAUD PREVENTION & SAFETY TIPS COGNIZANCE IN SOUTH AFRICAN BANKS. *Socioeconomica – The Scientific Journal for Theory and Practice of Socio-economic Development*, 1-15.
- Entersekt. (2021). *entersekt.com/5-tips-to-mitigate-digital-banking-payments-fraud*. Retrieved from [www.entersekt.com](https://www.entersekt.com/5-tips-to-mitigate-digital-banking-payments-fraud): <https://www.entersekt.com/5-tips-to-mitigate-digital-banking-payments-fraud>
- Epp, A., & Otnes, C. (2021). High-Quality Qualitative Research: Getting Into Gear. *Journal of Service Research*, 1-5.
- Financial Sector Conduct Authority. (2021, December). *Home>Regulated Entities>List of Regulated Entities and Persons*. Retrieved from [fsca.co.za/](https://www.fsca.co.za/): https://www.fsca.co.za/MagicScripts/mgrqispi.dll?APPNAME=Web&PRGNAME=List_Of_Registered_Insurers
- Herselman, M., & Warren, M. (2004). Cyber Crime Influencing Businesses in South Africa. *Issues in Informing Science & Information Technology*, 1-15.
- Josephson, A., & Smale, M. (2020). What Do you Mean by “Informed Consent”? Ethics in Economic Development Research. *Applied Economics Perspectives and Policy*, 1305-1329.
- Keith, T. Z. (2015). *An introduction to multiple regression and structural equation modeling (2nd edition)*. New York: Taylor and Francis.
- Knoke, D., Bohrnstedt, G. W., & Mee, A. P. (2002). *Statistics for social data analysis*. Itasca, Ill. : F.E. Peacock Publishers.
- Maluleke, W., Motseki, M. M., Mokwena, R. J., & Dlamini, S. (2021). The modus operandi of perpetrators for credit card. *Cogent Social Sciences*, 1-12.
- Manzoor, A. (2020). *Cognitive Analytics: Concepts, Methodologies, Tools, and Applications*. Pakistan: Bahria University, Pakistan.
- Maxwell, A. J. (2012). *Qualitative Research Design: An Interactive Approach*. United States of America: Library of Congress Cataloging-in-Publication Data.
- Mohottige, G., Sujeewa, M., Shukri, M., Yajid, A., Khatibi, A., Azam, S. M., & Dharmaratne, I. (2018). THE NEW FRAUD TRIANGLE THEORY - INTEGRATING ETHICAL VALUES OF. *International Journal of Business, Economics and Law*, Vol. 16, Issue 5, 1-6.
- Muhammad , S., & Kabir, S. (2016). *METHODS OF DATA COLLECTION*. Bangladesh: Book Zone Publication, Chittagong-4203, Bangladesh. Retrieved from <https://www.researchgate.net/publication/325846997>
- Murphy, M. (2016). Population definitions for comparative surveys in education. *Australian Council for Educational Research*, 1-33.
- Noble, H., & Heale, R. (2019). Triangulation in research, with examples. *Evidence Based Nursing*, 1-3.
- Pan, P. (2020). Ethics in Research and Publication. *Journal of Indian Association of Pediatric Surgeons*, 349–351.

- Pillay, E. (2015). *Big data analytics to combat cyber fraud in the South African banking sector*. Johannesburg.
- Radware. (2021, August 17). *Radware.com/security/ddos-knowledge-center/ddospedia/digital-fraud*. Retrieved from Radware.com: <https://www.radware.com/security/ddos-knowledge-center/ddospedia/digital-fraud>
- Rahi, S. (2017). Research Design and Methods: A Systematic Review of Research Paradigms, Sampling Issues and Instruments Development. *International Journal of Economics & Management Sciences*, 2-6.
- Riahi, Y., & Riahi, S. (2018). Big Data and Big Data Analytics: Concepts, Types and Technologies. *International Journal of Research and Engineering*, 1-6.
- Ronnie , L., & Ditshego, J. (2020). An assessment of perceptions concerning digital transformation at a South African commercial bank – a case of Anthropocene denial for the economy? *Social Sciences*, p687-p707, 21p.
- SABRIC. (2021). *sabric.co.za*. Retrieved August 17, 2021, from <https://www.sabric.co.za/media-and-news/press-releases/digital-banking-crime-statistics/>: <https://www.sabric.co.za/media-and-news/press-releases/digital-banking-crime-statistics/>
- SAFPS. (2021). *businesstech.co.za/news/technology/342057/big-increase-in-identity-fraud-cases-in-south-africa/*. Retrieved from businesstech.co.za: <https://businesstech.co.za/news/technology/342057/big-increase-in-identity-fraud-cases-in-south-africa/>
- Scalcău, A. (2021). Research Methods in Discourse Analysis: Quantitative, Qualitative and Mixed-Method Approaches. *Professional Communications and Translation Studies* , 1-10.
- Schoonenboom, J., & Johnson , R. (2017, July 05). How to Construct a Mixed Methods Research Design. 107-131. doi:<https://doi.org/10.1007/s11577-017-0454-1>
- Shrestha, N. (2020). Detecting Multicollinearity in Regression Analysis. *American Journal of Applied Mathematics and Statistics*, 39-42. doi:10.12691/ajams-8-2-1
- Swaen, B. (2015). Constructing a conceptual framework.
- Taherdoost, H. (2017). Determining Sample Size; How to Calculate Survey Sample Size. *International Journal of Economics and Management Systems*, Vol. 2, 1-3.
- The South African Insurance Association. (2021, November). <https://www.saia.co.za/index.php?id=1>. Retrieved from saia.co.za: <https://www.saia.co.za/index.php?id=1>
- TransUnion. (2021). *suspected-financial-services-digital-fraud-attempts-from-south-africa-rise-187-as-prevalence-of-digital-transactions-increase/*. Retrieved from transunion.co.za: <https://newsroom.transunion.co.za/suspected-financial-services-digital-fraud-attempts-from-south-africa-rise-187-as-prevalence-of-digital-transactions-increase/>
- Wolfe, D., & Hermanson, D. (2004). The fraud diamond: Considering four elements of fraud. *The CPA Journal*, 38-42.

Young, D. S. (2017). *Handbook of Regression Analysis*. Boca Raton, FL London New York CRC Press, Taylor & Francis Group.

APPENDICES

Appendix 1: Survey

Start of Block: Introduction

Dear Participant,

My name is Nonhlanhla Mahlangu and I am a Master of Business Administration (MBA) student at Wits Business School. As part of my research study, I am investigating a digital fraud strategy framework for banks and insurance companies in South Africa under the supervision of Dr. Oro Ufuo Oro.

I would like to invite you to participate in an online survey for my research study. The survey will take approximately 15 minutes to complete. Participants' confidentiality and anonymity are maintained as the survey does not request any personally identifiable information such as names or contact information. Participation is entirely voluntary and you may withdraw from the survey at any stage. Choosing to proceed and complete the survey will be considered as consent to participate.

If you have any questions about my research or this survey, please contact me at this e-mail address: 1168252@students.wits.ac.za. Alternatively, you can contact me on my cell number: +27 76 319 4461.

Thank you in advance for participating in the study.

Kind regards,

Nonhlanhla

End of Block: Introduction

Start of Block: Screening

Q1. Do you work in a bank or an insurance company?

☐ Yes (21)

☐ No (22)

Skip To: End of Survey If Q1. Do you work in a bank or an insurance company? = No

Q2. Are you an executive or non-executive member?

☐ Executive (1)

☐ Non-executive (2)

End of Block: Screening

Start of Block: Demographics

Q3. Which industry do you work for?

☐ Banking industry (1)

☐ Insurance industry (2)

Q4. Which one of the following roles best describes your position?

☐ C-Level Executive (e.g. CEO, CIO, COO) (1)

☐ Head/Executive Head of Business Unit (2)

☐ Middle Manager (4)

☐ Other (5) _____

Q5. Which of the following best describes your business function?

- ☐ Information Technology (IT) (1)
- ☐ Finance (2)
- ☐ Sales & Customer Service (3)
- ☐ Operations (4)
- ☐ Human Capital (5)
- ☐ Research and Development (6)
- ☐ Strategy and Innovation (7)
- ☐ Data and Analytics (8)
- ☐ Legal, Risk and Compliance (11)
- ☐ Digital (15)
- ☐ Marketing (16)
- ☐ Other (17) _____

End of Block: Demographics

Start of Block: Organisational Structure

Q6. In your organisation, do you have an executive responsible and accountable for digital fraud?

- ☐ Strongly disagree (1)
 - ☐ Disagree (2)
 - ☐ Somewhat disagree (3)
 - ☐ Neither agree nor disagree (4)
 - ☐ Somewhat agree (5)
 - ☐ Agree (6)
 - ☐ Strongly agree (7)
-

Q7. In your organisation, have you clearly defined roles and responsibilities of your digital fraud team?

- ☐ Strongly disagree (9)
 - ☐ Disagree (10)
 - ☐ Somewhat disagree (11)
 - ☐ Neither agree nor disagree (12)
 - ☐ Somewhat agree (13)
 - ☐ Agree (14)
 - ☐ Strongly agree (15)
-

Q8. In your organisation, do you have a cross-functional working group for digital fraud?

- ☐ Strongly disagree (9)
- ☐ Disagree (10)
- ☐ Somewhat disagree (11)
- ☐ Neither agree nor disagree (12)
- ☐ Somewhat agree (13)
- ☐ Agree (14)
- ☐ Strongly agree (15)

End of Block: Organisational Structure

Start of Block: Legislations and Regulations

Q9. Which of the following policies apply to your organisation?

Select applicable option(s)

- ☐ Fraud policy (1)
- ☐ Ethics policy (2)
- ☐ Risk policy (3)
- ☐ Digital or cyber fraud policy (4)
- ☐ Fraud prevention policy (31)
- ☐ Whistle-blowing risk policy (32)

Q10. Do government legislation and regulations have an impact on combating digital fraud in your organisation?

- ☐ Strongly disagree (12)
- ☐ Disagree (13)
- ☐ Somewhat disagree (14)
- ☐ Neither agree nor disagree (15)
- ☐ Somewhat agree (16)
- ☐ Agree (17)
- ☐ Strongly agree (18)

End of Block: Legislations and Regulations

Start of Block: Strategy

Q11. What percentage of your organisation's digital revenue is lost due to digital fraud?

- ☐ 0% (4)
 - ☐ 0 - 5% (5)
 - ☐ 5 - 20% (6)
 - ☐ 20 - 35% (7)
 - ☐ 35 - 50% (8)
 - ☐ 50% (14)
-

Q12. Is there a written digital fraud strategy document in your organisation?

- ☐ Strongly disagree (9)
 - ☐ Disagree (10)
 - ☐ Somewhat disagree (11)
 - ☐ Neither agree nor disagree (12)
 - ☐ Somewhat agree (13)
 - ☐ Agree (14)
 - ☐ Strongly agree (15)
-

Q13. Does your organisation conduct digital fraud risk assessments?

0 - They don't do this at all well

100 - They do this extremely well

0 10 20 30 40 50 60 70 80 90 100

Move the slider ()	
--------------------	--

Q14. Does your organisation have a risk-tolerance limit regarding digital fraud?

- ☐ Strongly disagree (27)
- ☐ Disagree (28)
- ☐ Somewhat disagree (29)
- ☐ Neither agree nor disagree (30)
- ☐ Somewhat agree (31)
- ☐ Agree (32)
- ☐ Strongly agree (33)

End of Block: Strategy

Start of Block: Technology

Q15. Does your organisation have the following technology in place for digital platforms? Please select one or more options that are applicable to your organization:

- ☐ Device Intelligence: To help customers in verifying identity, assessing and mitigating risk in real time, and improving customer experience (1)
- ☐ Behavioral Biometrics: To prevent identity-related digital fraud without disrupting users (2)
- ☐ Personal Identifiable Information: To identify customers by using information that, when used alone or in conjunction with other relevant data, can identify an individual (3)
- ☐ In-App messaging: To interact with digital platform users (4)
- ☐ One-time-pin: To authenticate or provide security for digital transactions (5)

Q16. Does your organisation use Artificial Intelligence (AI) technology for digital fraud (e.g. Biometrics, Face recognition)?

- ☐ Strongly disagree (9)
- ☐ Disagree (10)
- ☐ Somewhat disagree (11)
- ☐ Neither agree nor disagree (12)
- ☐ Somewhat agree (13)
- ☐ Agree (14)
- ☐ Strongly agree (15)

End of Block: Technology

Start of Block: Investigations

Q17. Does your organisation have a forensic or investigations department that proactively drive investigations for digital fraud?

- ☐ Strongly agree (37)
- ☐ Agree (38)
- ☐ Somewhat agree (39)
- ☐ Neither agree nor disagree (40)
- ☐ Somewhat disagree (41)
- ☐ Disagree (42)
- ☐ Strongly disagree (43)

End of Block: Investigations

Start of Block: Education and Awareness

Q18. Does your organisation drive digital fraud awareness and educational campaigns?

0 - They don't do this at all well

100 - They do this extremely well

0 10 20 30 40 50 60 70 80 90 100

Move the slider ()



Q19. Does your organisation share the latest information on new digital fraud scams to prevent fraud?

- ☐ Strongly disagree (26)
- ☐ Disagree (27)
- ☐ Somewhat disagree (28)
- ☐ Neither agree nor disagree (29)
- ☐ Somewhat agree (30)
- ☐ Agree (31)
- ☐ Strongly agree (32)

Q20. Does your organisation offer ongoing fraud awareness training?

- ☐ Strongly disagree (26)
 - ☐ Disagree (27)
 - ☐ Somewhat disagree (28)
 - ☐ Neither agree nor disagree (29)
 - ☐ Somewhat agree (30)
 - ☐ Agree (31)
 - ☐ Strongly agree (32)
-

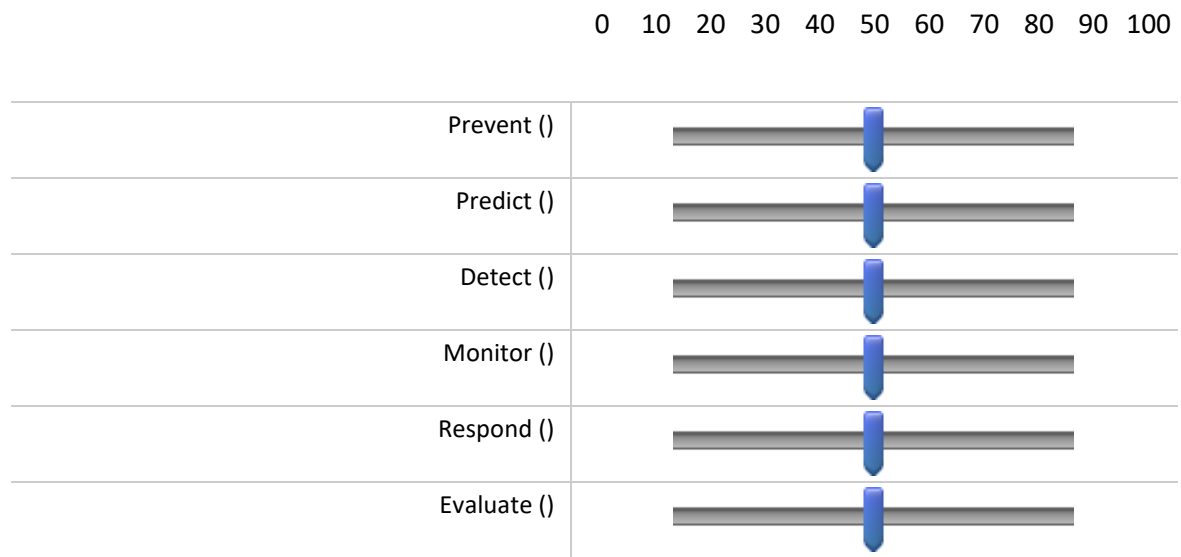
Q21. Are employees made aware of the organisation's position on digital fraud?

- ☐ Strongly disagree (26)
- ☐ Disagree (27)
- ☐ Somewhat disagree (28)
- ☐ Neither agree nor disagree (29)
- ☐ Somewhat agree (30)
- ☐ Agree (31)
- ☐ Strongly agree (32)

End of Block: Education and Awareness

Start of Block: Data and Analytics

Q22. Your organisation use big data for digital fraud in order to:
Indicate your choice by moving the slider.



Q23. Does your organisation use predictive and preventative models to prevent and predict digital fraud?

- ☐ Strongly disagree (9)
- ☐ Disagree (10)
- ☐ Somewhat disagree (11)
- ☐ Neither agree nor disagree (12)
- ☐ Somewhat agree (13)
- ☐ Agree (14)
- ☐ Strongly agree (15)

End of Block: Data and Analytics

Start of Block: Digital Fraud Amount

Q24. How much does your organisation lose as a result of digital fraud per annum?
Annual loss in Rands.

- ☐ Less than R500 000 (1)
- ☐ R500 000 - R1 000 000 (2)
- ☐ R1 000 000 - R 5 000 000 (3)
- ☐ R5 000 000 - R10 000 000 (4)
- ☐ More than R10 000 000 (5)
- ☐ Prefer not to say (6)

End of Block: Digital Fraud Amount

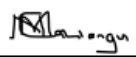
Appendix 2: Interview Guide

1. Demographics	Describe to me what your role is within your company?
	Describe to me what your business unit does?
2. Organisation/ Structure	In your organisation, have you clearly defined roles and responsibilities of the digital fraud team? (Bank or insurance participants only) and/or Describe if it is important for insurance and banking companies to clearly define roles and responsibilities of their digital fraud team?
	In your organisation, do you have a cross-functional working group for digital fraud? (Bank or insurance participants only) and/or In your view, describe if it is important for banks and insurance companies to have a cross-functional working group for digital fraud?
3. Legislations and regulations	In your organisation, do you have the following policies in place?

	<i>(Bank or insurance participants only)</i> and/or Describe if you think it is important for Banks and Insurance companies to have the below policies and if is it important to ensure that the policies are understood by staff members? 1. Group fraud policy document? 2. Ethics policy document? 3. Fraud prevention policy? 4. Cyber/Digital Fraud policy?
	Would you say that the government's legislations and regulations have an impact on banking and insurance companies?
4. Strategy	What percentage of your company's earnings could be attributed to digital fraud? ○ 0 – 5% ○ 5 – 15% ○ 15% – 25% ○ 25% – 35% ○ 35% – 45% ○ 45% – 55% ○ 55% + What, in your opinion, is an acceptable percentage loss in a financial company's earnings that can be attributable to digital fraud? <i>(Non-Bank or non-insurance participants only)</i>
5. Technology	Describe the systems that are in place on your digital platforms? <i>(Bank or insurance participants only)</i> and/or Describe if it is important for banks and insurance companies to have the following systems in place on their digital platforms? 1. Device Intelligence: Help customers in verifying identity, assessing and mitigating risk in real time, and improving customer experience. 2. Behavioral Biometrics: Prevent identity-related digital fraud without disrupting users. 3. Personal Identifiable Information (PII): Identify customers by using information that, when used alone or in conjunction with other relevant data, can identify an individual 4. In App messaging: Interact with users, both external customers or internal employees 5. One-time-pin for every transaction made

	6. Does your organisation use Artificial Intelligence (AI) Technologies for Digital Fraud (E.g. Biometrics, Face recognition)?
6. Investigations	Does your organisation have a forensic or investigations department that proactively drive investigations for digital fraud? <i>(Bank or insurance participants only)</i> and/or Describe the importance of having a forensic or investigations department that proactively drives investigations for digital fraud? Describe how your organisation drive proactive investigations for digital fraud.
7. Education and Awareness	Describe how your organisation drive digital fraud awareness and education campaigns internally? <i>(Bank or insurance participants only)</i> and/or Describe how financial companies can effectively drive digital fraud awareness and education internally? Describe how your organisation drive digital fraud awareness and education campaigns externally? <i>(Bank or insurance participants only)</i> And/or Describe how financial companies can effectively drive digital fraud awareness and education externally? Describe how your organisation share the latest information on new digital fraud scams used by fraudsters on digital platforms? <i>(Bank or insurance participants only)</i> and/or Describe how financial organisations could share the latest information on new digital fraud scams used by fraudsters on digital platforms?
8. Data and Analytics	Describe how your organisation use: 1. Big data to prevent digital fraud. 2. Analytic models to predict and prevent digital fraud across the customer life cycle <i>(Bank or insurance participants only)</i> And/or 1. Does big data play a role in preventing digital fraud and why? 2. Do analytical models help to predict and prevent digital fraud across for financial companies
9. Trends	Based on the different components discussed above, what are the latest trends when it comes to digital or cyber fraud (From a global perspective or SA)?

Appendix 3: Ethics Clearance Certificate

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/BA1168252/600 <i>This certificate is only valid with a legitimate ethics protocol number and signed by the Researcher (below).</i>		
This certificate is only valid if accompanied by formal permission from the relevant stakeholder(s).		
Project title	A digital fraud strategy framework for banks and insurance companies in South Africa	
Investigator / Researcher	Miss Cecilia Mahlangu	
Nature of Project	MBA (Research Article)	
Decision of the Committee	Approved, provided stakeholders and participants are guaranteed anonymity and confidentiality.	
Issue Date of Certificate	2021-11-14	
Expiry date	Date of submission of the project report	
Chairperson	Prof Anthony Stacey ☎ +27 11 717 3587 ☎ +27 82 880 4531 ✉ anthony.stacey@wits.ac.za 	
Declaration by Researcher		
<i>One copy must be signed by the Researcher and returned to the Chairperson of the Wits Business School Ethics Committee.</i>		
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	27 November 2021 Date:	

Appendix 4: Participant Consent Information (Online Survey)



The University of Witwatersrand, Johannesburg

Graduate School of Business Administration

2 St David's Place, Parktown, Johannesburg, 2193, South Africa
P O Box 98, WITS, 2050
Telephone: +27 11 717 3544
Facsimile: +27 11 717 3538
Website: www.wbs.ac.za

Dear Participant,

My name is Nonhlanhla Mahlangu and I am a Master of Business Administration student at Wits Business School. As part of my research study, I am investigating a digital fraud strategy framework for banks and insurance companies in South Africa under the supervision of Dr Oro Ufuo Oro.

I would like to invite you to participate in an online survey for my research study. The survey will take approximately 15 minutes to complete. Participants' confidentiality and anonymity are maintained because the survey does not request any personally identifiable information such as names or contact information. Participation is entirely voluntary. Choosing to proceed and complete the survey will be considered as consent to participate. You may withdraw from the survey at any stage.

If you have any questions about this research, please contact me at this e-mail address: 1168252@students.wits.ac.za. Alternatively, you can contact me on my cell number: +27 76 319 4461.

Thank you in advance for participating in the study.

Kind regards,

Nonhlanhla

Appendix 5: Participant Consent Information (Interviews)



The University of Witwatersrand, Johannesburg

Graduate School of Business Administration

2 St David's Place, Parktown, Johannesburg, 2193, South Africa
P O Box 98, WITS, 2050
Telephone: +27 11 717 3544
Facsimile: +27 11 717 3538
Website: www.wbs.ac.za

Dear Participant,

My name is Nonhlanhla Mahlangu and I am a Master of Business Administration student at Wits Business School. As part of my research study, I am investigating a digital fraud strategy framework for banks and insurance companies in South Africa under the supervision of Dr Oro Ufuo Oro.

I would like to invite you to participate in an interview for my research study. The interview will take approximately 30 minutes to complete. Participants' confidentiality and anonymity are maintained because the interview questions do not request any personally identifiable information such as names or contact information. Participation is entirely voluntary. I would also like to record the interview with your permission. This recording will be stored in a password-protected folder on my laptop. Only the researcher will have access to it, and it will be deleted after the completion of the research. You may withdraw from the survey at any stage.

If you have any questions about this research, please contact me at this e-mail address: 1168252@students.wits.ac.za. Alternatively, you can contact me on my cell number: +27 76 319 4461.

Thank you in advance for participating in the study.

Kind regards,
Nonhlanhla

Appendix 6: Participant Consent Form (Interviews)

Consent Form

A digital fraud strategy framework for banks and insurance companies in South Africa.

Researcher Name: Nonhlanhla Mahlangu

I, ..., agree to participate in this research project. The research study has been explained to me, and I understand what my participation will entail. I agree to the following:

Please mark relevant options with an X.

	Yes	No
I agree that my participation will remain anonymous	☐	☐

	Yes	No
I consent to the researcher using anonymous quotes in his or her research report.	☐	☐

	Yes	No
I agree that the interview may be audio recorded	☐	☐

	Yes	No
I agree that the information I provide may be used anonymously for academic purposes by other researchers after this project has concluded, subject to their own ethics clearance.	☐	☐

Signature:

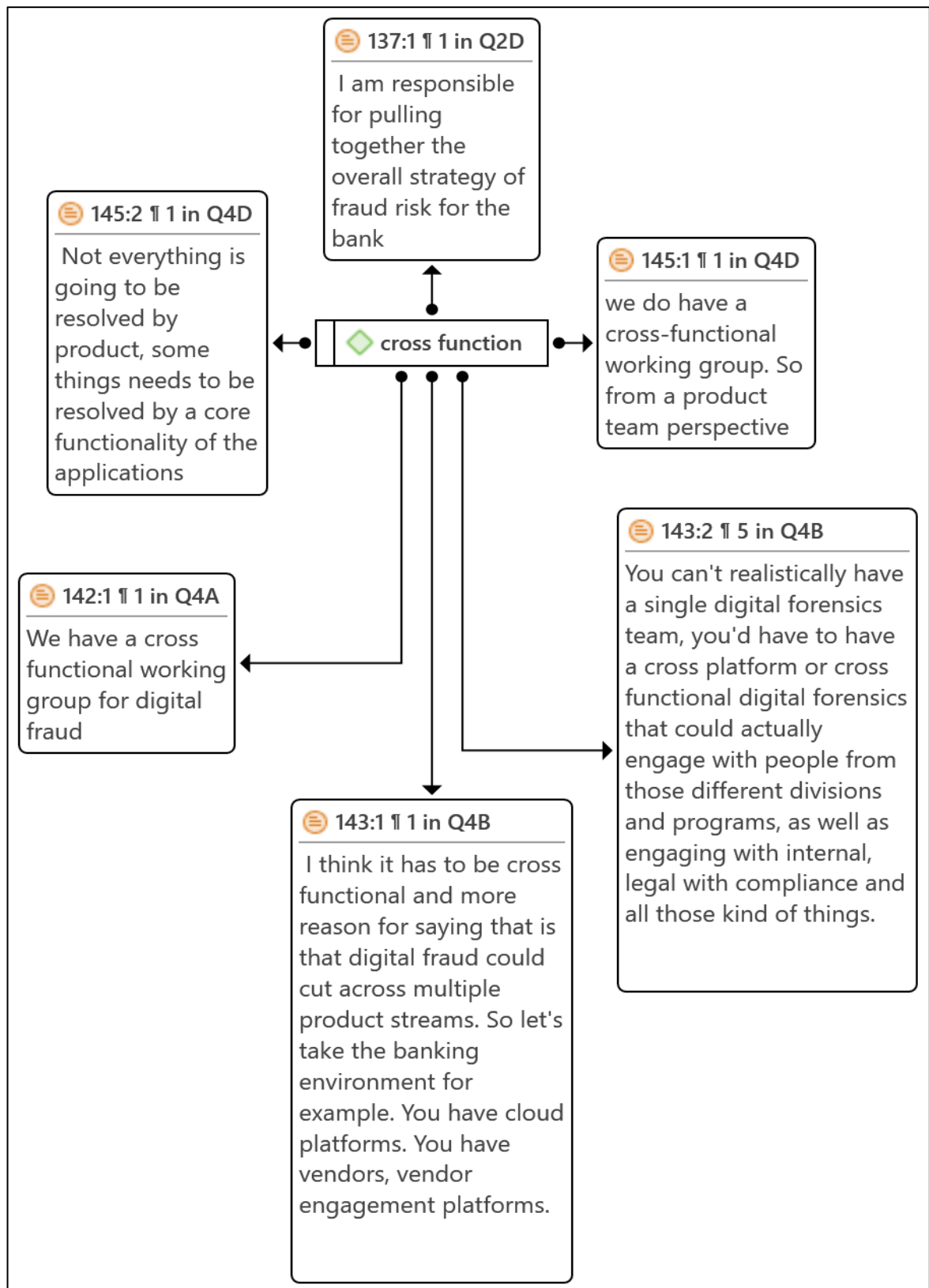
Name of participant:

Date:

Appendix 7: Correlation Matrix

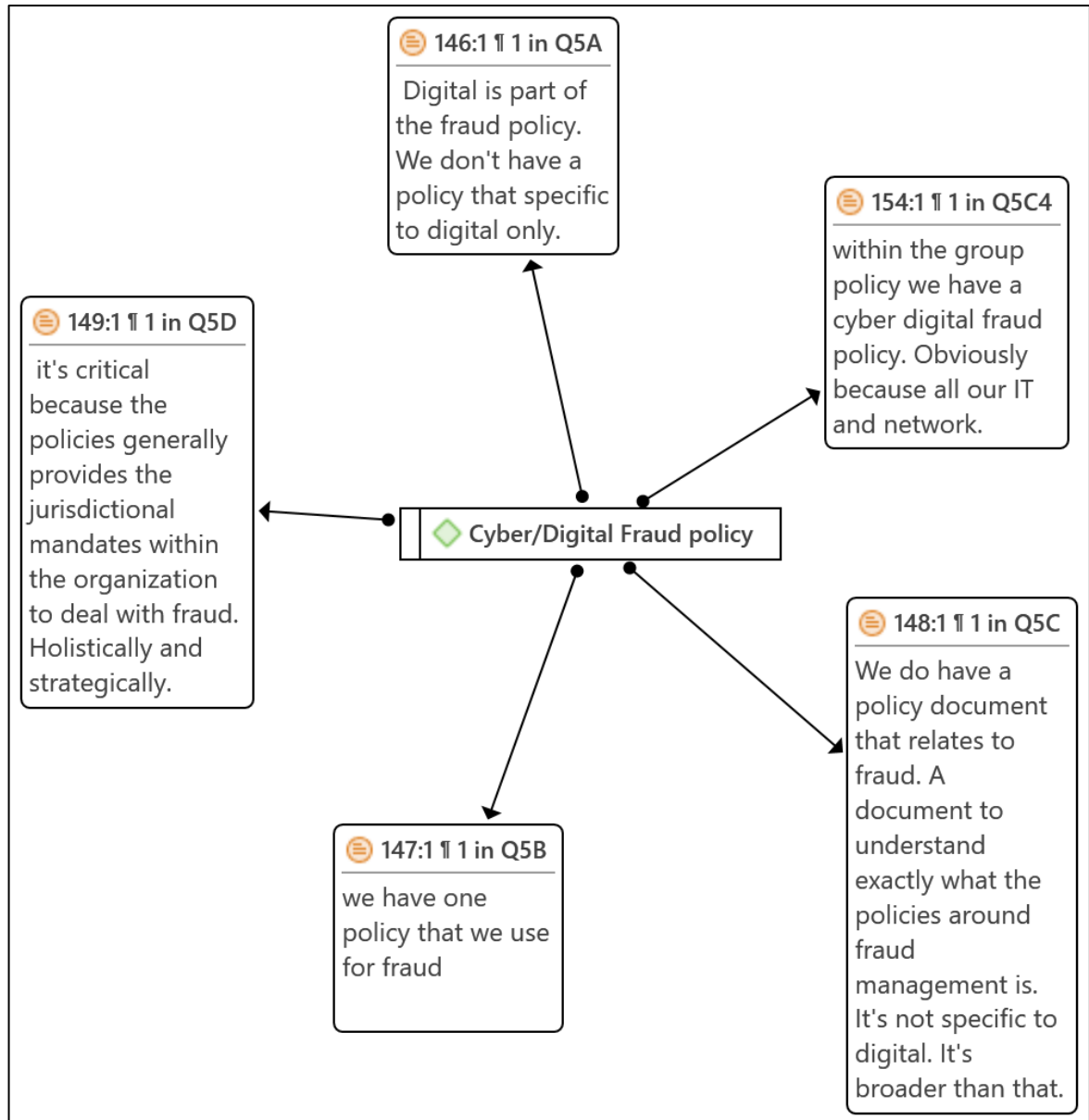
	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13_31	Q14	Q15	Q16	Q17	Q18_28	Q19	Q20	Q21	Q22a	Q22b	Q22c	Q22d	Q22e	Q22f	Q23	Organisati	Strategy	Technolog	Technolog	Investigati	Legislator	Legislator	Awareness	analytics
Q6	1.0000																															
Q7	0.7132	1.0000																														
Q8	0.6381	0.7857	1.0000																													
Q9	-0.0023	-0.0280	-0.0010	1.0000																												
Q10	0.4348	0.2022	0.2780	-0.0605	1.0000																											
Q11	0.1080	0.2462	-0.2073	0.1454	-0.1694	1.0000																										
Q12	0.5769	0.4622	0.7073	-0.1228	0.4170	-0.2631	1.0000																									
Q13_31	0.6639	0.6363	0.6604	-0.1509	0.2878	0.0409	0.7696	1.0000																								
Q14	0.4105	0.3178	0.4675	-0.1688	0.2795	-0.1900	0.4345	0.4955	1.0000																							
Q15	0.3020	0.1824	0.3491	0.1061	0.0782	-0.1232	0.3040	0.3378	0.2334	1.0000																						
Q16	0.5038	0.5064	0.4837	-0.2524	0.0682	0.1725	0.4714	0.6730	0.5241	0.4346	1.0000																					
Q17	-0.0917	-0.1710	-0.2799	0.0870	-0.1663	-0.0836	-0.2296	-0.1381	0.1522	0.0864	0.0700	1.0000																				
Q18_28	0.6660	0.5971	0.6640	-0.1180	0.3261	0.0281	0.6935	0.8573	0.6416	0.4683	0.7491	0.0345	1.0000																			
Q19	0.1405	0.0610	0.1976	-0.1938	0.2961	-0.2330	0.3928	0.2343	0.1403	0.2892	0.2763	0.0185	0.3449	1.0000																		
Q20	0.4395	0.3916	0.3542	-0.2393	0.1404	0.2089	0.3966	0.5157	0.4262	0.2132	0.6924	0.2387	0.6477	0.2858	1.0000																	
Q21	0.5816	0.5749	0.4093	-0.0521	0.1428	0.2384	0.3623	0.6133	0.5770	0.3457	0.7361	0.3414	0.6981	0.0818	0.6796	1.0000																
Q22_16	0.4752	0.4983	0.4915	-0.1007	0.3746	0.0511	0.5143	0.7024	0.5095	0.3144	0.6576	0.1845	0.7995	0.4127	0.6037	0.6827	1.0000															
Q22_17	0.4133	0.3769	0.3387	-0.2057	0.2932	-0.1140	0.2799	0.5055	0.4743	0.3340	0.5793	0.2684	0.5778	0.4164	0.4512	0.6176	0.7810	1.0000														
Q22_18	0.5467	0.5806	0.5335	-0.0575	0.2186	0.0682	0.4852	0.6918	0.3891	0.4035	0.7111	0.2026	0.7887	0.3954	0.6694	0.7287	0.8940	0.8056	1.0000													
Q22_19	0.5956	0.5621	0.5493	-0.1822	0.4388	0.0258	0.4217	0.6675	0.5448	0.3547	0.6659	0.1937	0.7550	0.2653	0.6414	0.6964	0.8257	0.8121	0.7996	1.0000												
Q22_20	0.4270	0.3359	0.3005	0.0660	0.3760	0.0236	0.2521	0.4479	0.5496	0.4451	0.4230	0.4380	0.6351	0.3330	0.4815	0.6710	0.7964	0.7245	0.7094	0.7788	1.0000											
Q22_21	0.4743	0.4184	0.3947	-0.0662	0.4071	-0.0493	0.3634	0.5783	0.5223	0.4265	0.5359	0.2940	0.7224	0.4232	0.5496	0.6426	0.8453	0.7781	0.7954	0.8094	0.8964	1.0000										
Q23	0.2637	0.2657	0.3257	-0.3050	0.0864	-0.0780	0.3372	0.5034	0.5039	0.3437	0.6942	0.3654	0.5904	0.2543	0.5639	0.6613	0.6334	0.6270	0.6624	0.6720	0.5378	0.4847	1.0000									
Organisati	0.8615	0.9237	0.9107	-0.0110	0.3368	0.0386	0.6548	0.7269	0.4473	0.3131	0.5527	-0.2075	0.7153	0.1518	0.4366	0.5732	0.5431	0.4159	0.6143	0.6313	0.3905	0.4748	0.3194	1.0000								
Strategy	0.6707	0.6336	0.6782	-0.1558	0.3060	0.0125	0.7952	0.9981	0.5364	0.3432	0.6787	-0.1339	0.8688	0.2478	0.5234	0.6196	0.7077	0.5095	0.6900	0.6717	0.4583	0.5844	0.5125	0.7357	1.0000							
Technolog	0.3020	0.1824	0.3491	0.1061	0.0782	-0.1232	0.3040	0.3378	0.2334	1.0000	0.4346	0.0864	0.4683	0.2892	0.2132	0.3457	0.3144	0.3340	0.4035	0.3547	0.4451	0.4265	0.3437	0.3131	0.3432	1.0000						
Technolog	0.5038	0.5064	0.4837	-0.2524	0.0682	0.1725	0.4714	0.6730	0.5241	0.4346	1.0000	0.0700	0.7491	0.2763	0.6924	0.7361	0.6576	0.5793	0.7111	0.6659	0.4230	0.5359	0.6942	0.5527	0.6787	0.4346	1.0000					
Investigati	-0.0917	-0.1710	-0.2799	0.0870	-0.1663	-0.0836	-0.2296	-0.1381	0.1522	0.0864	0.0700	1.0000	0.0345	0.0185	0.2387	0.3414	0.1845	0.2684	0.2026	0.1937	0.4380	0.2940	0.3654	-0.2075	-0.1339	0.0864	0.0700	1.0000				
Legislatio	-0.0023	-0.0280	-0.0010	1.0000	-0.0605	0.1454	-0.1228	-0.1509	-0.1688	0.1061	-0.2524	0.0870	-0.1180	-0.1938	-0.2393	-0.0521	-0.1007	-0.2057	-0.0575	-0.1822	0.0660	-0.0662	-0.3050	-0.0110	-0.1558	0.1061	-0.2524	0.0870	1.0000			
Legislatio	0.4348	0.2022	0.2780	-0.0605	1.0000	-0.1694	0.4170	0.2878	0.2795	0.0782	0.0682	-0.1663	0.3261	0.2961	0.1404	0.1428	0.3746	0.2932	0.2186	0.4388	0.3760	0.4071	0.0864	0.3368	0.3060	0.0782	0.0682	-0.1663	-0.0605	1.0000		
Awareness	0.6645	0.5943	0.6549	-0.1324	0.3283	0.0327	0.6926	0.8505	0.6413	0.4705	0.7663	0.0575	0.9975	0.3876	0.6857	0.7189	0.8137	0.6000	0.8078	0.7672	0.6519	0.7392	0.6100	0.7101	0.8625	0.4705	0.7663	0.0575	-0.1324	0.3283	1.0000	
analytics_	0.5311	0.5006	0.4716	-0.0957	0.3845	0.0013	0.4209	0.6525	0.5481	0.4181	0.6481	0.2945	0.7802	0.4096	0.6187	0.7374	0.9378	0.8881	0.9092	0.9132	0.9005	0.9370	0.6603	0.5552	0.6579	0.4181	0.6481	0.2945	-0.0957	0.3845	0.7987	1.0000

Appendix 8: Cross-functional Team



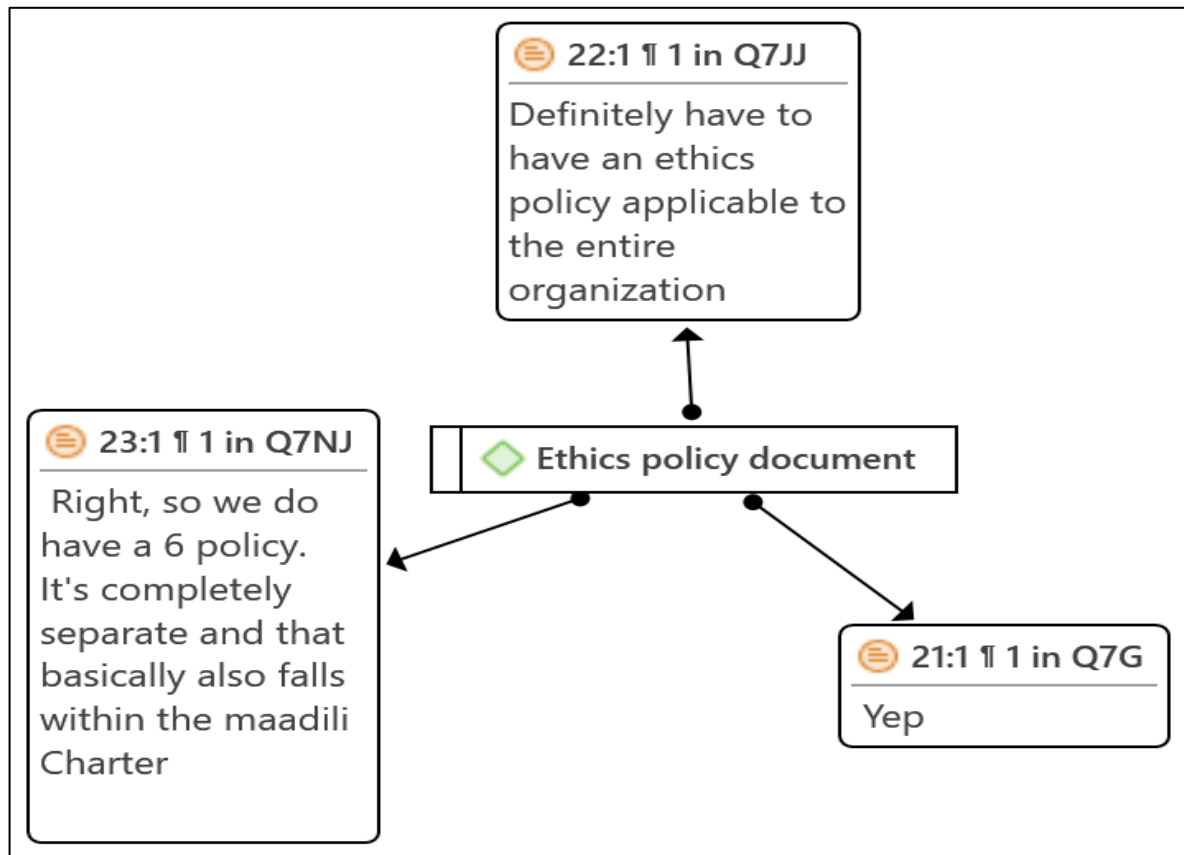
Source: ATLAS.ti output using the interviews dataset

Appendix 9: Fraud Policy Documents



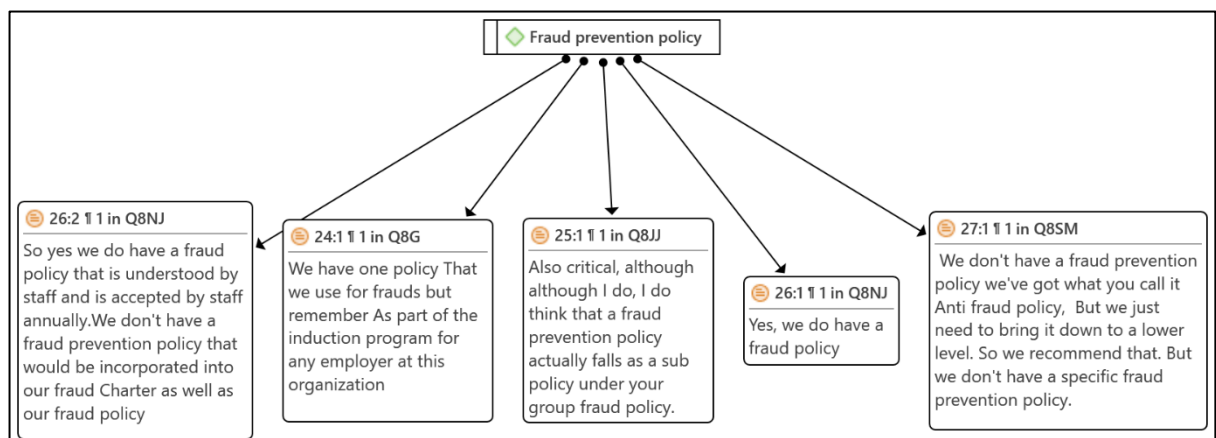
Source: ATLAS.ti output using the interviews dataset

Appendix 10: Ethical Policy Document, Fraud Prevention Policy



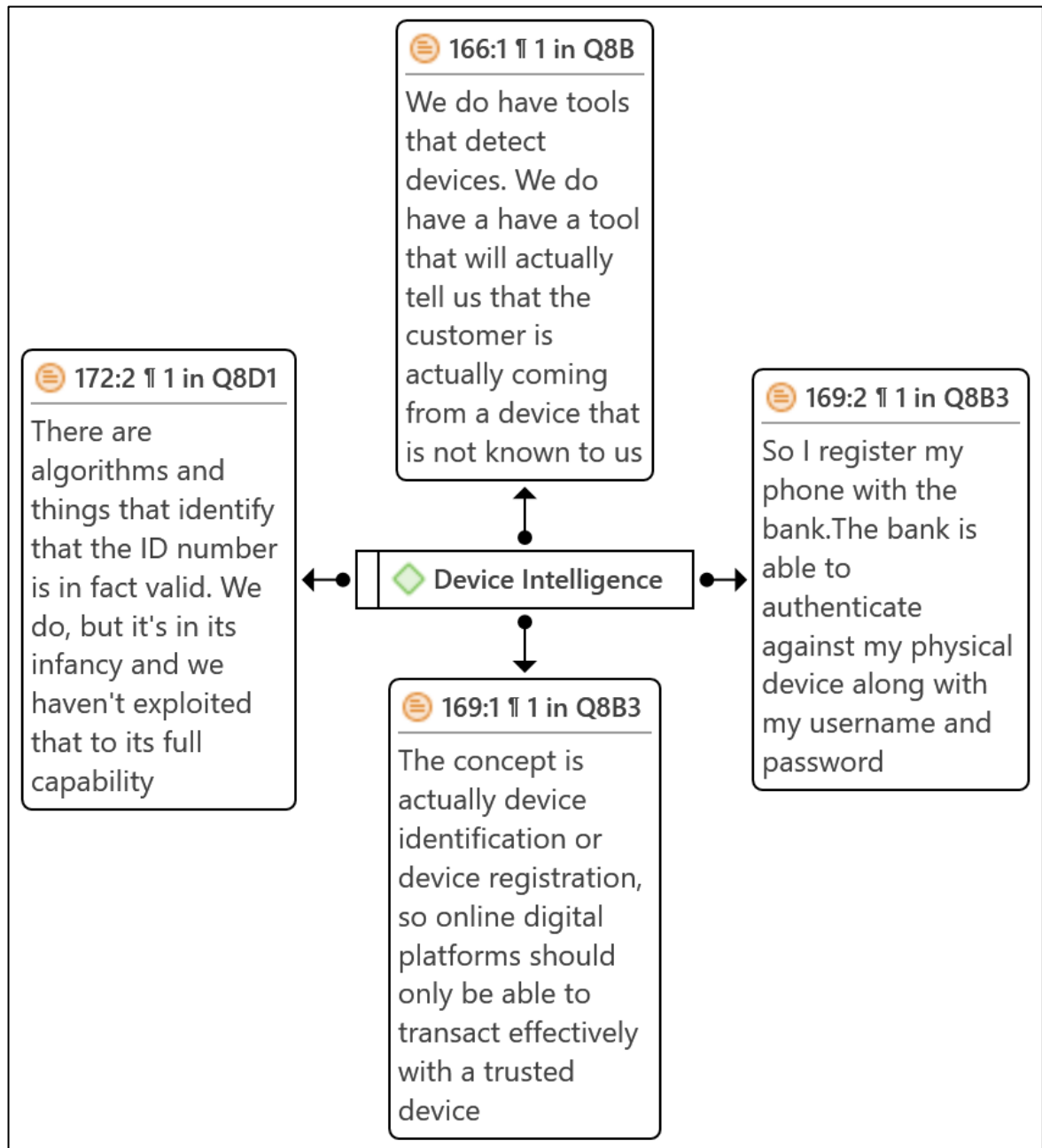
Source: ATLAS.ti output using the interviews dataset

Appendix 11: Fraud Prevention Policy



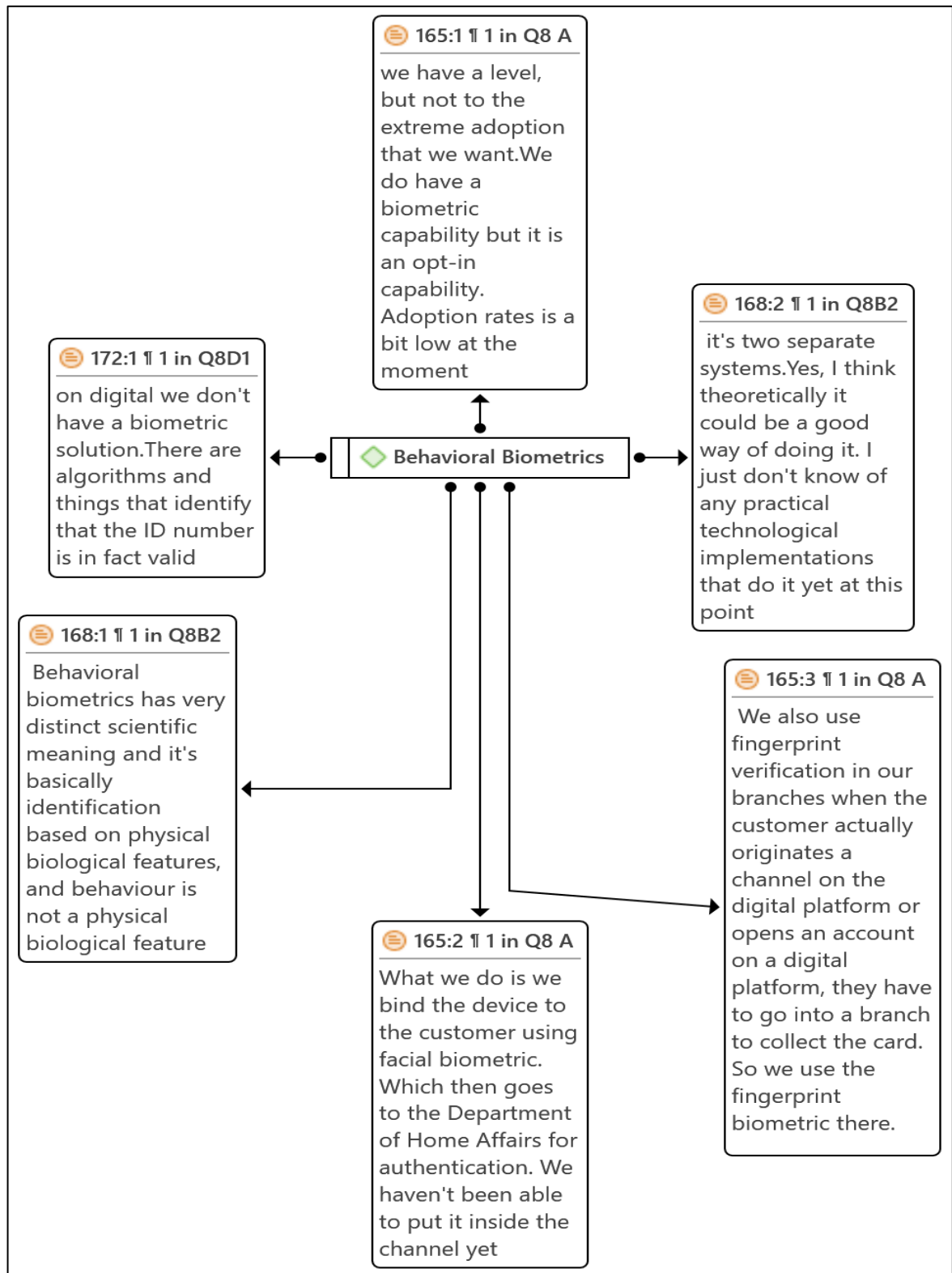
Source: ATLAS.ti output using the interviews dataset

Appendix 12: Digital Intelligence Responses



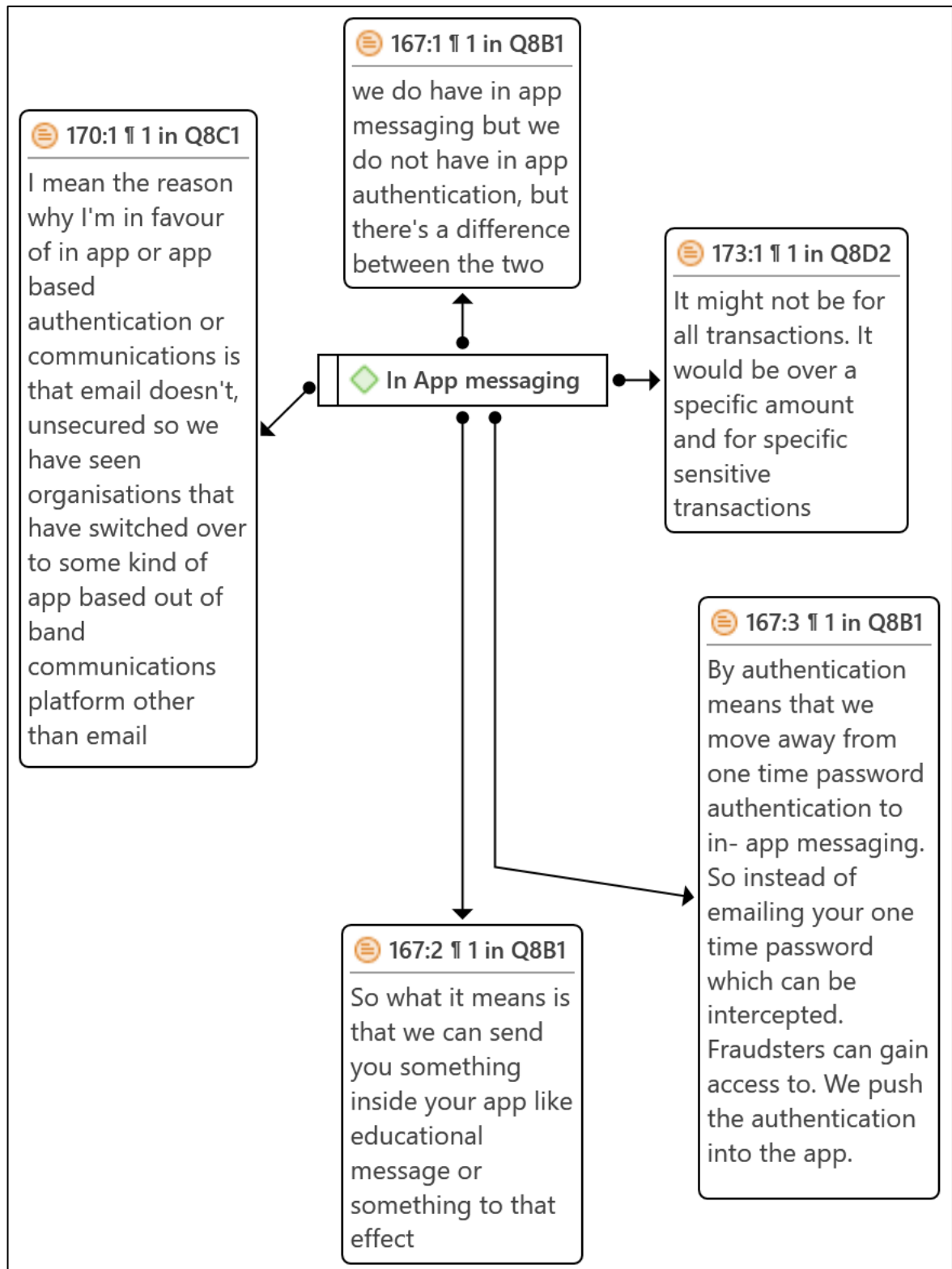
Source: ATLAS.ti output using the interviews dataset

Appendix 13: Responses on Behavioural Biometrics



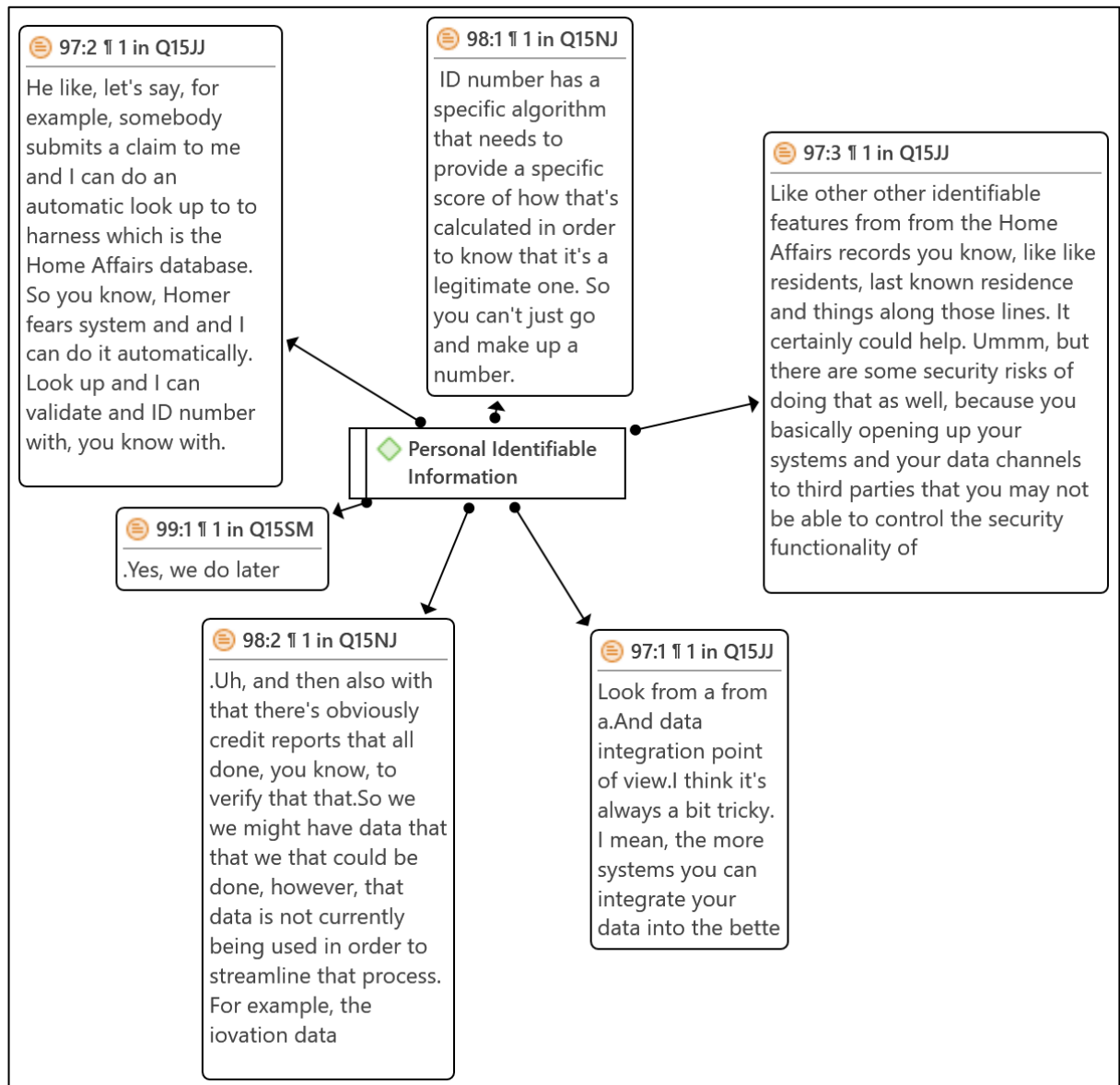
Source: ATLAS.ti output using the interviews dataset

Appendix 14: Responses on In-App Messaging



Source: ATLAS.ti output using the interviews dataset

Appendix 15: Responses on Personal Identification Information



Source: ATLAS.ti output using the interviews dataset