Cape Peninsula
University of Technology

THE INSTRUMENTATION OF DETECTIVE ANALYTICS FOR MITIGATING FINANCIAL CRIMES IN SOUTH AFRICAN INSTITUTIONS

by

NONTOBEKO NKOSINOMUSA BONGANGITHINI MLAMBO

Thesis submitted in fulfilment the requirements for the degree

Doctor of Philosophy in Informatics

in the Faculty of Informatics and Design

at the Cape Peninsula University of Technology

Supervisor: Prof Tiko Iyamu

Cape Town
November 2024

DECLARATION

I, Nontobeko Nkosinomusa Bongangithini Mlambo declare that the contents of this thesis represent my own unaided work, and that the thesis has not previously been submitted for academic examination towards any qualification. Furthermore, it represents my own opinions and not necessarily those of the Cape Peninsula University of Technology.

Signed: ____________________ **Date: November 2024**

ABSTRACT

The occurrence of financial crimes in South Africa has been significantly high. This is because many financial institutions conduct their operations through online, digital platforms. Digital operations in financial institutions increasingly rely on digital platforms due to the high demand for real-time quick services. This results in generating unprecedented data. Organisations use the data to make informed decisions, which increases the significance. The reliance on data has made financial institutions adopt and use tools such as detective analytics. However, the implementation of detective analytics remains challenging to individuals and organisations at large. The challenges are attributed to a lack of understanding of the factors that influence the implementation of detective analytics. There are concerns that the current data analytics tools being used by financial institutions have gaps and loopholes. Consequently, financial crimes are often identified only after their occurrence.

This study aimed to develop a tool that can be used to implement detective analytics to mitigate financial crimes. In achieving this aim, the researcher followed the case study approach using a South African financial institution as a case. The organisation was selected with a set of criteria. Qualitative research methods involving interpretive and semi-structured interview techniques were used to gain an in-depth understanding of the factors influencing financial crimes in South African financial institutions. The study employed the subjective approach from the interpretive perspective to gain insights into how detective analytics can be applied to mitigate financial crimes in financial institutions. Semi-structured interviews were conducted with business and information technology (IT) specialists. Also, the participants were selected using a set of criteria. The interviews stopped at a point of saturation, which means that no new information was forthcoming. Additionally, existing documents were gathered and used to complement the interview data. The university (CPUT) and the organisation's ethics, including participants' consent, guided the data collection.

The data was analysed using the four moments of translation actor-network theory (ANT as a lens to guide the data analysis. The theory was selected primarily for three reasons. Firstly, it focuses on translation, required to understand how meanings are associated with events and processes in mitigating financial crimes. Secondly, ANT enables an understanding of how actor networks are consciously formed, which helps to determine the formation of groups responsible for mitigating financial crimes in the organisation. Thirdly, ANT's mantra "follow the actors" was employed to follow the actors, from humans to non-humans, helping to gain a deeper understanding of why things happened in the ways they did in mitigating financial crimes in the organisation. From the analysis, seven factors were found to influence the use of detective analytics to mitigate financial crimes in organisations. The factors are as follows;

(1) Collaboration; (2) Corroboration; (3) Internalisation; (4) Externalisation; (5) Digitalisation; (6) Organisational structure; and (7) Integrated analytics.

Activity theory (AT) was used as a lens to guide the interpretation of findings. The interpretation revealed the links between the influencing factors (findings) including their attributes. Based on the influencing factors, the links, and the attributes, a framework was developed, which can be used to guide the adoption and implementation of detective analytics to trace, track, and prevent financial crimes in financial institutions in South Africa.

The study contributes to both business and academic domains from theoretical, practical, and methodological perspectives. Theoretically, the relationships between the influencing factors are established. Practically, organisations can develop policy and governance frameworks to prevent financial crimes, based on the influencing factors. Methodologically, the application of ANT and AT advances the use of sociotechnical theories in detective analytics.

ACKNOWLEDGEMENTS

I wish to thank:

- The Lord almighty, sengiyabala nkosi okuhle ongenzele khona, Philippians 4:13.
- To my late mother maMlambo Nikiwe Sthandesonke Virginia, this is what we both wanted.
- Shaped and sharpened by the best, my Professor Tiko Iyamu. Thank you for everything and most importantly for being patient with me throughout the journey.
- To my friends and my colleagues in the research forum, thank you for walking with me until the end.
- Lastly, to my kids Luthando and Luniko, thank you for being my inspiration.

DEDICATION

BoMlambo, Gubhuza, Mfula kawuwelwa owelwa zinkonjane zona ezindizela phezulu ngamaphiko. Bo Sishange sama Mabhedla. This doctoral degree is the first ever in my family, I want to dedicate it to my lineage. To my gran mother Ndaba'uyizwephi maFakazi, wena olalelwa izidalwa.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE
INTRODUCTION

1.1. Introduction

Financial institutions play a very vital role in the economy of any country. Financial institutions include banking agencies that assist individuals and organisations with carrying out transactions at both national and international levels (Ericson, 2021). The transactions include exchanging forex and assets from small to large volumes (Sunio & Mendejar, 2022). Some of the transactions have severe implications and consequences for the actors or the representing agents involved. For example, when a transaction goes wrong on a large scale, an entire organisation can be declared liquidated, which affects the livelihoods of the employees and others connected with the organisation. Therefore, it is critical to always guide against wrong transactions by being precautionary with the enabling facets, which are primarily people, data and technology.

Financial institutions rely on data for processing millions of transactions daily (Hasan & Rizvi, 2022). The data is enabled and supported using information technology (IT) solutions (Bataev, 2018). Furthermore, the manipulation, use and management of the data and IT solutions are carried out by people (Sahar et al., 2019.). Thus, financial institutions continue to build the security and protection of their assets and finances around these three facets. According to Li et al. (2020), financial institutions analyse data to gain a better understanding, make better financial decisions and help prevent the processing of suspicious transactions. Despite the preventative, detective, precautionary and security measures, processes and transactions are often in danger because of fraudulent activities from unprecedented circumstances (Yamen et al., 2019). Some of the activities are from internal and external entities and agents, including conscious and unconscious human actions. In the last ten years, South Africa has been one of the countries in the world most hit by financial crime (Kempen, 2020). Achim et al. (2021) argue that financial crime is double in low-income countries than it is in high-income countries. This could be attributed to the sophistication of preventative, detective, and other security measures in high-income countries, using IT solutions (Hope, 2020). Some financial crimes are detected by financial institutions (Gombiro et al., 2015). There are loopholes in the current methods and approaches, hence, the rate of financial crime in South Africa is increasing. Thus, a different mechanism is required to advance protection and security against financial crime in the country. This should allow and enable early detection of the crime before and as it happens, using the most appropriate mechanism such as detective analytics.

Detective analytics is in the family of data analytics, which includes diagnostics, descriptive, predictive, and prescriptive analytics (Vanani & Shaabani, 2021). Data analytics are widely used to combat financial crimes, and the most used analytics are predictive, prescriptive, and detective analytics (Menezes et al., 2019). Although there is closeness and a bit of overlap among the analytic tools (Lee et al., 2022), detective analytics uniquely focuses on identifying a problem in data, as and when it occurs (Menezes et al., 2019; Poornima & Pushpalatha, 2020). However, not many financial institutions use and know how to fully utilise the capabilities of detective analytics (Liu et al., 2021). Thus, this study sets out to examine and propose instrumentation of detective analytics for mitigating financial crime activities before and as they occur.

1.2. Background to the research

Relatively, the rate of financial crime in South Africa is very high when compared to other developing countries, particularly in the African continent (Hope, 2020). As a result, the South African government has tried various approaches to combating financial crimes in financial institutions. In the early 1990s, South African financial crime laws were improved to limit and combat financial crime activities (De Koker, 2007). More than a decade later, the situation has not eased; instead, it has increased. Hope (2020) cites state capture as evidence of financial crime and argues that until corruption channels such as embezzlement, theft, bribes, kickbacks, money laundering, and illicit financial flows are thoroughly investigated financial crime will continue to increase. In 2021, during the lockdown caused by Covid-19, which resulted in more reliance on online transactions, financial crime in South Africa increased by 15.1% (Ferreira & Koko, 2022).

The perpetrators of financial crimes in organisations are either internal or external personnel. From the internal perspective, the crimes are usually intended or unconscious (human error) by employees who have access to internal procedures and data, while the external factors include fraudsters, phishing and money laundering (Nakajima, 2007). The increase in financial crime is due to the emerging technologies that institutions adopt to enhance processes (West & Bhattacharya, 2016). Thus, there is a need to explore how detective analytics can be used as a mechanism to detect financial crime.

1.3. Research problem

Like many organisations, financial institutions depend on data for their strategic and operational activities. Unfortunately, the data includes processes which are continually infiltrated or manipulated, consciously by actors of criminal activities, and unconsciously by human errors (Akinbowale et al., 2020). Some of these crimes are so severe that the organisation is affected and may shut down, which inevitably has an impact on the livelihood of employees. Thus, institutions are constantly exploring and employing tools and approaches to mitigate financial crimes, which is prohibitive to business continuity. Thus, IT solutions are increasingly relied upon for remedy.

Despite IT security solutions and preventative tools such as the Financial Intelligence Centre Act (FICA), 2001; Banks Act, 1990; and Inspection of Financial Institutions Act, 1998 that have been deployed in layers, for mitigation purposes, financial crimes are on the increase in South Africa (Chitimira & Ncube, 2021; Sutherland, 2017). According to White (2018), “South Africa’s rate of reported economic crime remains significantly higher than the global average rate of 49%”. Consequently, many institutions continue to lose income to crime, which affects their sustainability and competitiveness. Another negative effect is that the affected institutions suffer reputation damage, which takes considerable time to recover from (Kshetri, 2019). These highlighted problems derail economic development and growth and affect individuals’ job security in the country. Thus, it is critical to find a fresh and more sophisticated solution to mitigating financial crimes for South African institutions.

1.4. Aim, objectives and questions

The aim and objectives of the research are presented as follows:

1.4.1. Research aim

The research aims to develop a framework that can be used to guide the implementation of detective analytics, to mitigate financial crimes.

1.4.2. Research objectives

In achieving the aim of the study as stated above, the following objectives were formulated:

i. The first objective is to understand how financial crimes happen in South African financial institutions and, thereafter, examine the current preventative and mitigative measures.
ii. To investigate how the detective analytics tool can be deployed to trace, track, and prevent financial crime in a financial institution.
iii. Based on objectives i and ii, a framework is developed to define and enable the implementation and use of detective analytics to mitigate financial crimes.

1.4.3. Research questions

The main question is: How can a framework be developed to enable the implementation of detective analytics to mitigate financial crimes in South African institutions?

1.4.4. Research sub-questions

The research sub-questions are as follows:

i. How are financial crimes committed and prevented or mitigated in South African financial institutions?
ii. How can the detective analytics tool be implemented to mitigate financial crimes in South African institutions?
iii. How can a framework be used to define and enable the implementation and use of detective analytics?

1.5. Literature review

This section presents the literature reviewed. It focuses on the core aspects of the study, which are financial crime in institutions and detective analytics. In addition, it reviews theories of actor-network theory (ANT) and activity theory (AT) that underpin the study is conducted.

1.5.1. Financial crime in Institutions

Most financial institutions rely on data, and the growth of data is drastic throughout the whole world (Bataev, 2018). Hasan et al. (2020) state that hundreds of millions of financial transactions occur in financial institutions each day and all these transactions lead to data creation. In this age of innovation and machine learning, data is seen as one of the most vital contributors to decision-making for most financial institutions. This being said, financial institutions have been targets for financial crimes both internally and externally (Yamen et al., 2019); internally by individuals who have access to transaction data and externally by individuals or organisations that target specific individuals' information to commit financial crimes. Financial institutions have seen a high rise in financial crimes over the past ten years which negatively impacts the development and reliance on information systems (Hope, 2020). Achim et al. (2021) argue that financial crime is double in low-income countries than it is in high-income countries. South Africa has been one of the leading countries exposed to financial crime (Kempen, 2020).

Financial crime is a widespread problem and has been reported to be very aggressive in African countries due to the high rate of poverty. The economic development minister in South Africa has claimed that over 76,000 jobs are lost every year due to financial crime (Hope, 2020). The South African government has tried its best to implement strategies to combat crime in general and these strategies also include laws regulating financial crime (De Koker, 2007; Kshetri, 2019). Macdonald (2019) states that financial crime activities such as money laundering have been considered the new way of making a living for most South Africans and a very profitable business to most. According to Van Niekerk (2017), most South African financial institutions have experienced a much higher rate of financial crimes due to the high demand for online transactions. Notwithstanding that most institutions have implemented technological enhancements to combat financial crime, Coetzee (2018) argues that technology is the main driver of financial crime.

1.5.2. Detective analytics

The use of data analytics has grown exponentially in the financial sector (Cockcroft & Russell, 2018). This can be attributed to its strengths of accurate reporting, cost reduction, enhanced decision making and operational benefits (Alsghaier et al., 2017; Ifenthaler, 2017; Wang & Hajli, 2017 Lazarova-Molnar; Mohamed & Al-Jaroodi, 2018). Data analytics in the financial sector creates opportunities to advance financial management for both customers and organisations (Giebe et al., 2019; Nobanee, 2021). Andriosopoulos et al. (2019) state that most financial problems that exist can be solved by examining the available data, which can be done through the use of data analytics. However, some researchers argue that the advancement of data analytics in the financial sector has not been thoroughly explored (Samuel, 2017; López-Robles et al., 2019; Sun et al., 2019). This being said, the most explored data analytics methods in the financial sector are, descriptive analytics, diagnostic analytics, predictive analytics and prescriptive analytics. However, detective analytics, in particular, has little to no research conducted in finance literature.

Detective analytics focuses on data analysis, like other tools such as descriptive, diagnostic, predictive, and prescriptive analytics. Descriptive analytics is used to understand what occurred in the past using historical data (Janakiraman & Ayyanathan, 2021). Diagnostic analytics focuses on historical data to gain a deeper understanding of the reason behind certain outcomes (Balali et al., 2020); hence, it is mostly used to build insights into why certain events occurred in the way they do (Deshpande et al., 2019). Predictive analytics is used to determine patterns and themes to understand what could happen soon (Jeble et al., 2018; Selvan & Balasundaram, 2021). From an organisation’s perspective, De Jesus Liriano (2019) states that to predict is to forecast a problem or a solution.

For many years, financial institutions have been using data analytics to derive patterns that lead to financial criminal activities (Ravi & Kamaruddin, 2017; Andriosopoulos et al., 2019; Derindere Köseoğlu et al., 2022). Fosso Wamba (2017) states that data analytics help to collect relevant data to access and integrate the data in providing reports of deeper insights into business operations and production. Thus, like other sectors, the use of data analytics has enhanced and enabled the financial sector to make better decisions (Ranjan & Jeyanthi, 2021). Increasingly, many organisations can use data analytics to explore and visualise data to a simple representation that can be easily understood by both users and managers (Khedr et al., 2017).

Despite the benefits that data analytics offers organisations, the financial sector continues to experience an increase in financial crimes (Holzenthal, 2017; Yeoh, 2019). Detective analytics is used to diagnose and detect a problem immediately as and when the problem occurs (Raeesi Vanani & Majidian, 2021). However, not many financial institutions use and know how to fully utilise the capabilities of detective analytics (Liu et al., 2021). Therefore, detective analytics should be critically explored in the financial sector to help combat crime within the institutions.

Among other things, detective analytics is used by organisations to detect fraudulent activities (Abdallah et al., 2016). To detect means to discover and identify a problem before it occurs. The use of detective analytics is not only advantageous for future purposes but also to detect traces and track incidents using historical data (Sun et al., 2011). Menezes et al. (2019) describe detective analytics as the combination of predictive analytics and prescriptive analytics in the sense that it forecasts and recommends solutions to problems as and when they occur. Thornton et al. (2013) state that fraud detection is used mostly to detect unknowns and known unknowns. Verma et al. (2017) emphasise the need for financial institutions to adopt effective fraud detection techniques such as detective analytics to reduce the number of fraud instances. The use of detective analytics is a needed mechanism for financial institutions due to most processes being data-driven (West & Bhattacharya, 2016).

1.5.3. Underpinning theories

This study is underpinned by two sociotechnical theories which are actor-network theory (ANT) and activity theory (AT). Considering the focus of this study, they are considered to be more suitable for this study. The theories are discussed in the remainder of this section. The theories are selected based on three main reasons. First, the nature of the study requires a socio-technical view. Second, in fraudulent financial activities, negotiations occur between humans, technologies, or humans and technology actors. One of the main focuses of ANT is understanding negotiation shifts among actors, consciously or unconsciously (Callon, 1986). Third, AT connects (or links) activities with humans through rules in their use of tools. Similar to ANT and its shifting negotiation, no other theory focuses on episodic linking events. Fourth, without a complementary use of the ANT and AT, there would be a gap, either in the analysis of the data or interpretation of the findings. Iyamu (2021) provides a comprehensive justification and offers a guide for employing AT and ANT complementarily.

1.5.3.1. Actor-Network theory

The ANT is a sociotechnical theory used by researchers to explain the relationship between humans and non-human objects (Couldry, 2008). Sage et al. (2011) further state that ANT is mostly focused on understanding how human and non-human actors are involved with non-human things. ANT was created by Michel Callon and Bruno Latourin in 1981. The theory aimed to determine how actors play a role in a network and vice versa (Gao, 2005). According to Walsham (1997), an actor network is formed immediately when the actors have aligned interests. The actor network is mostly formed unconsciously by actors not even being aware that they have formed one (Latour, 1996). The actor network focuses on how networks are built and maintained and what makes the network dissolve (Michael, 2016; Shim & Shin, 2016).

Applying ANT allows the researcher to follow the actors in their heterogeneous networks. This is because the theory offers methodological steps in the activities, actions, and interactions between actors in a network (Callon, 1986; Heeks & Stanforth, 2015). According to Iyamu (2021:73), "ANT provides a platform which allows for the analysis of both human and non-human interaction in a network. This means that ant is a resource for understanding the actions of humans". Lefkowitz (2022) draws on ANT to trace information pathways that enable humans to access actions and connect with needed resources. Kumar and Tissenbaum (2022) employ ANT to provide an underutilised post-humanist lens to understand the creation of collaborative connections between action-based interactions.

Another strength of ANT that was critically useful in this study is the concept of translation. Translation in ANT is the process of creating relations to things that were not previously related (Lezaun, 2017). The moment of translation occurs immediately when the actors' interests are aligned with their actor network (Walsham, 1997). The use of ANT has gained popularity in areas of IS research, such as the adoption of technology, in environments that include healthcare, engineering, finance, and education. ANT is mostly used in IT studies to understand the technology innovation process. (Shim & Shin, 2016). However, its coverage is not comprehensive enough in the context of this study because the theory does not implicitly focus on rules and division of labour. Thus, the activity theory is used for interpreting the findings.

1.5.3.2. Activity theory

The AT is a sociotechnical theory that originates from the discipline of psychology (Iyamu & Shaanika, 2019). Based on its focuses, it has been increasingly applied in information systems/information technology (IS/IT) studies over the last three decades and it is within the same frame that it was applied in this study (Nardi, 1996). According to Iyamu (2021), AT has been applied in studies over 3 million times. The theory is primarily applied in IS/IT studies to understand and evaluate the use of technologies within organisations (Kaptelinin & Nardi, 2018). Karanasios et al. (2018) argue that AT contributes mostly to the field of IS/IT because of its ability to create a relationship between fundamental components of IS/IT solutions, such as tools, subject (humans), rules (policies and regulations), and context (environment).

According to Ettema (2018), AT assists in studying how humans behave when using specific tools.

The theory consists of a model, which is commonly applied in IS/IT studies. It is referred to as the AT model, shown in Figure 1.1. The AT model seeks to understand the relationship between actors and how an activity (technology) is discovered through the AT components (Kaptelinin & Nardi, 2018). As shown in Figure 1, from the AT perspective, the relationship is discovered through its components which are tools, subject, rules, community, division of labour and the object, which is the outcome (Nardi, 1996). The components fortify the theory as a lens for examining and gaining a deeper understanding of the phenomenon being studied.

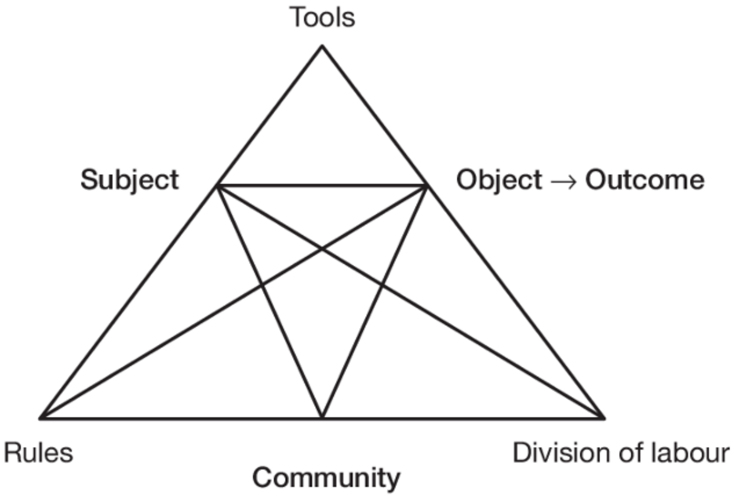

Figure 1.1: Activity theory model
(Nardi, 1996)

The tools can be anything such as software and hardware used by an individual or organisation to carry out an activity, including combating financial crime (Bertelsen & Bødker, 2003). The subject, as defined by Iyamu (2020), is a living being, which can either be an individual or a group of individuals. Rules, in the context of AT, are described as control mechanisms for individuals' activities (Engeström, 2001), which can be used to detect financial crimes in an organisation. In AT, a community consists of different individuals with common interests (Barab et al., 2004), such as financial crime perpetrators, victims, and anti-crime units. The division of labour seeks to understand the role each individual plays in the process of executing an activity (Engeström, 1999). The object leads to the outcome of an activity (Kaptelinin & Miettinen, 2005).

1.6. Research design and methodology

This section introduces the research design and methodology applied in this research, which is comprehensively discussed in Chapter 4. The methodology begins with philosophical assumptions, which lead to the research approach, research methods, research design, data collection technique, and data analysis technique selected for the research.

1.6.1. Philosophical assumption

In this research, assumptions are made, which are aligned to existing philosophies such as epistemology and ontology. This is not new, in that Endjala (2022) suggests that philosophical assumption is used in research as assumptions to guide inquiries. In IS research, two types of philosophical assumptions are common, namely, ontology and epistemology. This research follows the ontology and epistemology assumptions because the former is about the reality of existence (Brown, 2017; Neuhaus, 2017) and the latter focuses on gaining knowledge (Hájek & Hartmann, 2010; Titchen & Ajjawi, 2010), which are core aspects of this research.

In ontology, there are many realities to the existence of artefacts (Walliman, 2017), such as events and technology (Poli & Seibt, 2010). The events and realities of this study are the existence of financial institutions, financial crimes, and detective analytics. Ontologically, detective analytics is understood and viewed from different perspectives. For example, detective analytics was used with the Internet of Things (IoT) to generate new insights (Empl & Pernul, 2023). Another reality is that detective analytics has been used to obtain accurate predictions by organisations (Menezes et al., 2019). Also, there are various ways or approaches to the implementation or adoption of detective analytics. This includes the use of frameworks, policies, and models (Pramanik et al., 2016; Broeders et al., 2017; McKee, 2017). Some of the approaches have been employed by organisations across the world.

Based on an assumption, a position (stance) is taken. In this research, the ontological stance is subjectivism. This is because it allows the researcher to employ their reasoning and interpretations (Coats, 1983), which is required in this study. After all, there is no universal 'fit' in providing the solution. Thus, subjectively, the study induces how to implement detective analytics to mitigate financial crimes through instrumentation. From the epistemology perspective, subjectivism is the stance for this research. Primarily, this is because it allows different interpretations, which enables learning and gaining knowledge from various standpoints (Walsham, 2006; Titchen & Ajjawi, 2010; Tolmen, 2020).

1.6.2. Research approach

Of the existing research approaches, deductive (Hellstrand & Breckwoldt, 2016), inductive, and abductive (Buqa & Fung, 2019), the inductive approach was followed based on the aim and objectives of the study. The approach allows the researcher to induce their reasoning into the field of study and find solutions to a problem (Thomas, 2006). Thus, instrumentation can be induced towards mitigating financial crime within the financial institutions in the country.

1.6.3. Research methods

The most applied research methods in information systems studies are qualitative (Gerring, 2017), quantitative (Apuke, 2017), and mixed methods (McCusker & Gunaydin, 2015). The qualitative research method is selected for this study because it allows the use of natural language to describe data within context (Gerring, 2017). Bergman and Coxon (2005) argue that qualitative studies are subjected to the quality of the research questions, research objectives, data collected, the findings, and interpretation derived from the data. Thus, the method determines the research design, data collection techniques and analysis selected for the study.

The qualitative research method is preferred as it allows the researcher to be biased in offering meaningful insights into the phenomena. Qualitative research methods allow for the study to establish relationships between components as well as the social aspect of the phenomena being studied (Sofaer, 1999). The use of the qualitative research method allows for subjectivism which enables the researcher to provide an analysis based on their own judgement, providing an independent opinion based on what they understood of the data that informed their analysis (Crang, 2003). Being subjective is based on the researcher interrogating the phenomena with probing questions to understand the why, who, how, when, where and what happened behind certain behaviours, and interactions. (Nguyen et al., 2021).

The study is based on the occurrence of financial crimes and aims to understand and interrogate individuals both from business and IT to understand the nature of these crimes. Financial crimes happen in many organisations and these crimes have different perspectives which can be viewed differently based on one's understanding of them. The occurrence of financial crimes has many elements that need to be unpacked and understood. The enablers and the preventative measures need to be understood. This may be subjective. Gerring (2017) states that the biggest advantage of a qualitative research method is allowing the researcher to conduct the analysis and express it in natural language.

1.6.4. Research design

The case study approach was used for this study as described and explained by Yin (2015). The case study is most appropriate for this study because of its naturalistic approach (Hollweck, 2015). Smith (2020) states that the case study approach allows the researcher to perform investigations on case activities, in a real-life setting. Suryani (2008) argues that the case study approach enables an instance, where an individual or an organisation is being observed, to understand and analyse phenomena.

Organisations were used as cases in this study. A preliminary investigation was conducted to understand the organisations that are using detective analytics or are aware of the tool. One South African organisation (financial institution) was selected. A set of criteria was formulated and used to select the organisations. The set of criteria includes: (i) the organisations must be aware of detective analytics; (ii) the organisations must be willing to voluntarily participate in the study; and (iii) the organisations must be based in the province in which the researcher lives, for proximity purposes. Thus, a preliminary investigation was conducted to ascertain and select the organisation.

1.6.5. Data collection

Qualitative data was collected within the organisation selected as a case by following the case study approach (Al-Najran & Dahanayake, 2015; Yin, 2015). From the qualitative method perspective, the semi-structured interview technique was employed for the data collection. This is because the technique allows open-ended questions, which enable conversation between the interviewer (researcher) and interviewees (Magaldi & Berler, 2020). Another benefit is that the process allows clarification of subjects, terminologies, and questions, which enhances the quality of interview data (Qu & Dumay, 2011; Iyamu, 2018). The interview questions (guidelines) were aligned with the research questions.

The data collection process was guided by ethics. Ethical clearance was obtained from the University (CPUT). Additional ethical clearance was obtained from the institution that participated in the study. The participants (interviewees) were selected using a set of criteria. The criteria included but were not limited to (i) employee in the finance or IT department or division of the organisation; (ii) must have experienced crime in the organisation; (iii) must be knowledgeable about detective analytics; and (iv) must be part of the unit or department that provides, supports or manages mitigation solution. The interviews were held one-on-one with the participants at their preferred locations. The interview sessions were recorded with a physical tape recorder or through online platforms such as Zoom or Microsoft Teams. From the participants, the researcher requested permission to record the interview conversation. The data collected was stored in the institutions' access-controlled data management system. The CPUT data management plan was completed and used to manage data collected for the study.

1.6.6. Data analysis

Data analysis is defined as the process of coding, cleaning, translating and reorganising data (Islam, 2020). The process of coding and cleaning the data means that the data collected through interviews was separated per interview participant and coded to differentiate the participants. The participants are kept anonymous as per the ethical clearance declaration.

The data was thereafter cleaned to remove any words that did not add meaning to the sentences and for any grammatical errors. The collected data was thereafter ready for use in the data analysis section through translation. The interpretive approach was employed in the analysis. The analysis was guided using ANT as a lens. The findings from the data analysis were interpreted using AT. The theories are discussed in detail in the literature review section. From the discussion, the focus of the theories is different.

ANT was used to understand how networks of actors are consciously or unconsciously formed. This allows actors to be followed to establish their roles in the processes and activities in finance transactions within the organisation. The use of ANT helps to gain insights into how negotiation shifts among actors, during finance transactions within the organisation. This includes gaining a deeper understanding of the relationship that exists between the actors in the process of executing financial transactions. Through its use for interpretation of the findings, AT helps to gain a better understanding of how financial transactions that lead to crime are connected. This helps to determine how humans interpret and apply rules in carrying out financial transactions in the organisation. This includes how various tools (such as detective analytics) are applied to mitigate financial crime.

1.7. Ethical consideration

The study focused on one financial institution as a case for this research. As stated in the data collection, ethical clearance will be obtained from CPUT and the institutions. Due to ethical reasons, the financial institution is referred to using a pseudonym; Nikiwe Federal Finance (NFF). A pseudonym is defined as when an individual or an organisation being referred to is kept anonymous (Gerrard, 2021). The participants for the study were selected from the IT and business departments, focusing on the financial crime department. The participants from the IT department were contacted as the research is focused on the use of detective analytics which would be introduced to the business by IT. Therefore, the IT individuals are critical for this study to understand the current measures they have in detecting, tracking and tracing financial crimes.

The financial crime department is also very critical for this study to understand the types of financial crimes that currently happen, and how they are being prevented or mitigated currently by the business. This will help understand how a detective analytics tool can be implemented to mitigate financial crimes in South African institutions. Participants interviewed for the study did so voluntarily and only participants who know detective analytics and financial crimes partake in the study.

The researcher reached out to both the IT department and the financial crime department to arrange interviews with the financial crime team and the data analytics team to get their view on financial crimes and the use of detective analytics in their space. The criteria used for selecting the participants were clearly defined and discussed in the data collection section above.

1.8. Significance of the study

The study is significant for organisations and academia. Organisations' business and IT people will find this study important and benefit from it. The business people will learn and understand how a detective analytics tool can assist the organisation in tracking and tracing financial crimes. This will enable and assist in getting confidence that the organisation as a whole will lose less money due to the tool assisting them to find loopholes using the detective analytics tool. The IT people will also benefit significantly by being able to use a tool driven by detective analytics to manage and support the financial crime department in tracking and tracing crimes. Furthermore, the IT department can learn about detective analytics and enhance its capabilities to detect financial crimes through the proposed instrumentation.

Academically, this study will be significant practically and theoretically. Practically, an instrument using detective analytics will be developed that will assist organisations to prevent, track and trace financial crimes as and when they happen. Theoretically, there is a gap in the body of knowledge on the use and application of detective analytics. This study will therefore help researchers understand more about the use of detective analytics and its capabilities. At the time of the study, there seems to be no clear indication of how financial institutions utilise detective analytics to prevent financial crimes. This study will help to define and enable the use of detective analytics in organisations. This instrument can be used by any financial institution that has a financial crime department, especially banking institutions.

1.9. Delineation of the study

The study focuses on the use of detective analytics, specifically from a South African financial institution perspective. This means that the study does not include all developing countries and is primarily focused on the South African context. However, the study can be applied in other financial institutions in developing countries that utilise detective analytics as a mechanism to detect financial crime. As discussed in detail above in the literature review section, the detective analytics family has other tools such as descriptive analytics, diagnostic analytics, predictive analytics, and prescriptive analytics. However, for this study, only detective analytics will be used as a tool to detect financial crimes as and when they happen.

1.10. Contribution of the study

This study contributes from theoretical, practical, and methodological perspectives. Theoretically, this study will add to the existing body of knowledge in the areas of data analytics, information management, and information systems. Currently, there is limited literature about detective analytics across the globe, to be more specific, from developing countries' perspectives. The study is intended to benefit all financial institutions as all are exposed to financial crimes across the globe, more specifically in developing countries like South Africa, which is challenged with technological advancement in detecting financial crimes when they happen.

Practically, the instrument that will be developed is a major contribution to the advancement of IT solutions in organisations. The instrument can be used to trace, track, and monitor financial transactions in an organisation. This infused enablement of the instrument will lead to mitigating financial crime in an organisation. Currently, no tool across the globe uses detective analytics to detect financial crimes as and when they happen. This tool will be developed in South Africa but can be used and deployed across the globe.

Methodologically, complementary uses of ANT and AT have not been applied or tested in sensitive areas such as the data analytics phenomenon. The complementarity advances the collaboration between social-technical theories (ANT and AT) and IT solutions (data analytics).

1.11. Conclusion

This study is primarily focused on developing a tool to implement detective analytics, which can be used to mitigate financial crimes. The research objectives and questions are formulated based on the problem. Comprehensively, the relevant literature is reviewed. The most appropriate technical methods and approaches will be selected as proposed in this document. The significance and contributions of the study are relevant to both the academic and business domains. The document is well structured and adheres to the University template.

CHAPTER TWO
LITERATURE REVIEW

2.1. Introduction

This chapter presents the literature review that was conducted. The review is based on the objectives of the study as stated in Chapter One. This means that the review focuses on the key aspects of the study, which are financial crime in organisations, the adoption of technology to mitigate financial crime, and detective analytics for financial crime. Also covered in the chapter are the theories.

The remainder of this chapter is structured into five main sections. The first section focuses on financial crime. In the second section, financial crimes in organisations are discussed. The adoption of technology to mitigate financial crimes is covered in the third section. Detective analytics for financial crime is discussed in the fourth section. Finally, the chapter is summarised in the last section.

2.2. Financial crime

Financial crime happens in organisations in different ways (Hasham et al., 2019). Hence, it is described or defined in various ways. Mentari and Hudi (2022) described financial crime as a crime conducted to steal money for financial gain, which results in financial loss for either an organisation or an individual. Van Niekerk and Phaladi (2020) defined financial crime as an illegal act of defrauding an individual or organisation of money. Although used interchangeably, white-collar and corporate crimes are also fraudulent events that are described as financial crimes (Donning et al., 2019). Due to the boundaryless nature of financial crime, it is an international problem, as it continues to affect individuals and organisations in direct or indirect ways (Uniamikogbo et al., 2019). Thus, it is viewed in some quarters as a global pandemic that challenges the financial sector because of increasing financial losses (Avortri & Agbanyo, 2020).

Some of the losses have detrimental effects on many organisations. See Bowron and Shaw (2007), where the impact of financial crimes on individuals, organisations, and governments is comprehensively explained. Even though Bowron and Shaw's (2007) study was almost two decades ago, the challenges remain. For example, as recently as two years ago, Contreras and Ghosh (2022) revealed that in some instances, financial crime has caused many financial institutions to fail, liquidate, or disrupt their growth or competitiveness. Owing to the consequences of financial crimes, mitigating measures are continuously explored and deployed. Despite these measures, financial crime continues to increase across the world. Statistically, criminal activities in the areas of finance have increased exponentially over the past ten years (Khotsa, 2019; Murphy et al., 2020). Different reasons can be attributed to the increase. Zweni and Yan (2022) linked the increase in financial crimes to ignorance of financial laws and management practices in many countries, including South Africa.

Also, the digital age increased financial crimes through cybercrime, which is mostly associated with social media and online links that are easily accessible (Marelino, 2022). The most common type of financial crime is cryptocurrency fraud, which is conducted by individuals to scam people of their money (Trozze et al., 2022). In various countries, there are bylaws, regulations, rules, and standards to control, manage, and monitor financial transactions and mitigate crimes (Scott, 2020). Yet, the crimes persist, increasingly, mostly in developing countries such as South Africa. Thus, Tansu (2023) states that it is critical to understand the complexity of financial crime compliance, including the risks associated with activities, processes, and transactions. Almakhfor and Norton (2021), therefore, argue the criticality of the need to regularly detect and report financial crimes in organisations. This includes an understanding of access to systems, enabling applications, and unauthorised information that are exploited to execute fraudulent acts (Koval et al., 2019).

In South Africa, financial crime is increasing and overwhelmingly affecting many individuals, groups, and organisations (Akinbowale et al., 2024). Thus, financial crime is being studied as a socio-economic issue as it affects both the social behaviour and economics of the country (Diremelo, 2020). Chitimira and Ncube (2020) argue that due to the low income earned and high cost of living in South Africa, some people turn to crime to make ends meet. Furthermore, Mazorodze (2020) argues that financial crime in South Africa is highly linked to unemployment. The highest concerns that lead to high crime rates in South Africa are inequality and poverty (Cook, 2020).

The South African government has promulgated laws and adopted approaches to mitigate financial crimes. Despite the measures, financial crime is increasing in the country (De Koker, 2007). Akinbowale et al. (2024) argue that many technologies have been adopted over the years such as the use of continuous auditing, firewalls, and data mining; however, the financial crime rate persists. Some of the adopted approaches are the use of information technology (IT) solutions such as artificial intelligence (AI), which enables machine learning, deep learning, and data analytics (Chitimira & Ncube, 2021). Hope (2020) states that various laws such as the Anti-money laundering policy and Anti-financial crime policy have been endorsed to mitigate or minimise financial crimes in South Africa. Furthermore, the South African government implemented the Electronic Communications and Transactions (ECT) Act, primarily, to protect organisations against theft, forgery, and other types of financial crimes (Dagada, 2024).

2.3. Financial crime in organisations

Financial crimes are happening in various forms and through different means in organisations across the globe, including South Africa. Avortri and Agbanyo (2020) revealed that it has been noted by the regulator that fraudulent transactions have led to a huge loss of money for many financial institutions across the globe. South African banks experience financial crime, mostly through digitisation and automation creative initiatives, often aided by human interactions with the system (Hasham et al., 2019). As a result, various mitigative controls are employed, yet the challenges persist (Marxen, 2022). Many organisations rely on anomaly detection to detect and prevent financial crimes as and when they happen (Nicholls et al, 2021). Some financial institutions have adopted methods to better understand the various tools and techniques the perpetrators use to defraud them (Achim et al., 2021; Teichmann & Falker, 2021).

Financial crimes do not only affect big organisations; they also do happen to small and medium enterprises. The crimes experienced by organisations are committed by internal or external actors (individuals or groups) (Siregar et al., 2020). Many of the crimes are committed through interactions with the organisation's system and between actors (Albrecht et al., 2019; Othman et al., 2023). Vozniuk et al. (2020) suggest that interaction with the system allows the perpetrators to steal or defraud organisations using electronic means or physical cash.

The organisations most affected by financial crime are in developing countries (Amara & Khlif, 2018; Saddiq & Abu Bakar, 2019). According to Achim et al. (2021), this is because the controls enabled by IT solutions to mitigate financial crimes in developed countries are much more advanced than those employed in developing countries. This could be attributed to various factors, such as a lack of knowledge about the application of some IT solutions deployed to mitigate financial crimes (Merlonghi, 2010; Sigetova et al., 2022). De Koker and Goldbarsht (2022) argue that some developing countries lack the knowledge and experience of how to apply certain tools and methods in adopting fast-paced technologies, such as detective analytics, for mitigating financial crime. Somehow, this explains why South Africa is among the countries most affected by financial crime globally (Ehiane et al., 2023).

2.4. Adoption of technology to mitigate financial crime

Financial institutions are constantly generating data, which consists of transaction and customer information using IT solutions (Gaumer et al., 2016). Also, organisations are constantly exploring IT solutions that can assist them in measuring, monitoring, and mitigating financial crimes (Dowsley, 2021). The exploits of vast IT solutions result from sensitive information stored and used by the banking sector (Choto, 2018). However, Murphy et al. (2020) argue that regardless of the high rate of financial crimes, some banks are still using manual processes and are slow in adopting technology to mitigate financial crimes. Thus, Ivanyuk (2023) suggests that the rapidity of events requires organisations to be swift in their responsive actions to allow customers to confidently transact businesses online.

Various technologies (IT solutions) have been developed and adopted to mitigate financial crimes in different sectors, locally and internationally (El Mouaaouy, 2018). Despite the continuous innovation in the development of IT solutions, perpetrators continue to explore loopholes in them. Also, the adoption of some of the IT solutions is challenging. These challenges form one of the reasons why internal employees or external agents infiltrate the system (Saxena et al., 2020). Whether from internal or external sources, the perpetrators interact with the system to find loopholes, based on which they execute their crimes. Powelson (2022) suggests that the rate at which finances are increasing will make it a global pandemic. Along the same line, Jasinski et al. (2023) argue that financial crimes, from both internal and external perspectives, are a global pandemic because they affect everyone (Jasinski et al., 2023).

In most instances, IT solutions (systems and applications) are exploited by internal staff members who know the rules and how to violate them (Supriyanto et al., 2023). Teichmann and Wittmann (2022) explain that most of the decisions taken by financial crime suspects are based on their knowledge of the environment or influenced by the culture of the organisation. Many organisations across the world have tried different approaches in their attempts to prevent financial crimes. However, there are still loopholes, either in the technologies or the implementation of the solution. In addition to IT solutions, policies are adopted to govern and ensure controls mitigating financial crimes. Despite these measures and efforts, there remain challenges from both human and technological perspectives (Donning et al., 2019). As a result, perpetrators gain access to internal applications and systems by interacting with employees of an organisation (Supriyanto et al., 2023).

Adopting technology to mitigate and monitor financial crimes has posed many challenges for financial institutions, notwithstanding the advantages (Suryono Budi & Purwandari, 2020). There has been rapid adoption of technologies to mitigate and monitor financial crimes in recent years (Holt et al., 2022). Some of these technologies are artificial intelligence and machine learning software (tools), used to detect financial crimes (Kute et al., 2021). This includes blockchain technologies, which allow only authorised individuals to decrypt and read transaction data (Frizzo-Barker et al., 2020; Patel et al., 2022).

However, whenever a technological solution emerges, some financial institutions are reluctant to operationalise (adopt, implement, and use) it, due to security concerns (Nangin et al., 2020). Hussain et al. (2021) allude that a policy-enforced framework should be adopted by financial institutions to ensure that their security and privacy measures are addressed. This type of framework provides a guide within context, to test and evaluate an IT solution.

2.5. Detective analytics for financial crime

The financial crime department is one of the most sensitive areas in financial institutions due to the complexity of storing and processing customers' confidential data (Hasham et al., 2019). Many financial institutions have adopted various advanced technologies such as machine learning and artificial intelligence in their attempts to address the complexity while processing both structured and unstructured data (Gilchrist, 2022). However, the adoption of advanced technologies such as detective analytics to prevent financial crimes as and when they occur has not been explored (Suzumura et al., 2019). The financial systems being used to store and process customer data are always at risk of being manipulated for financial crimes (Ünvan, 2020). Therefore, it is critical to explore a more advanced tool, such as detective analytics, to combat financial crimes, especially in this big data era (Cheng et al., 2021).

The term detective analytics is often referred to as advanced analytics in some quarters (Aliguliyev et al., 2016). In this study, the term detective analytics is consistently used. The primary focus of detective analytics is to predict and prescribe improvements for an organisation based on its transactional data (Menezes et al., 2019). Empl and Pernul (2023) state that detective operations are meant to know about an incident based on certain variables that should alert the organisations of any anomalies occurring at a given moment. However, the 'variables and given moment' must be programmed into the system, within context, for detective purposes. This is one of the challenges some organisations encounter because it requires deep knowledge and expertise, which they often lack (Ara et al., 2024).

Notwithstanding the challenges, financial institutions are increasingly adopting analytics tools, to improve insights, management, and reporting of their data, for better decision-making. Rouhollahi (2021) states that the adoption of technologies such as analytics tools by financial institutions is to identify and predict potential financial crime activities. Regardless of its criticality, many financial institutions either lack the knowledge of detective analytics or how to implement it. Consequently, perpetrators find loopholes in the systems. Singh and Best (2019) alluded that tools do exist to report suspicious activities and detect them; however, the detection and reporting of these activities happen after the crimes have been committed and it is too late for recovery.

Although using detective analytics allows organisations to understand the present financial crime activities and predict what can happen shortly (Weller et al., 2023), the mechanism for doing so remains challenging. Hence, a framework or instrumentation approach is needed to guide the implementation and use of detective analytics to mitigate financial crimes. The framework or instrumentation will assist in intrusion detection to mitigate financial crimes as and when an anomaly is recognised (Empl & Pernul, 2023). The existing data analytics techniques enable organisations to understand what, when, where, why, and how something happened (Runkler, 2020). Currently, there seems to be no mitigative control or tool in place for financial institutions to detect financial crimes as and when they happen.

Various challenges are associated with adopting and implementing detective analytics. Menezes et al. (2019) argue that most organisations do not know how to fully use detective analytics for fraud prevention, detection, and defence. Using detective analytics to prevent financial crimes can be inaccurate if the reason for the crime is due to a conflict of interest which is not visible through the data (Pramanik et al., 2017). Hoelscher and Shonhiwa (2021) argue that for detective analytics to be fully functional and operate as intended, there should be controls and rules in place to identify anomalies. The use of detective analytics can easily be associated with machine learning where an instrumentation is being taught how to identify anomalies for ease of prevention and defence. There may be uncertainties which detective analytics might not know how to report and remediate (Yong, 2019).

2.6. Conclusion

The literature review is comprehensive and covers all the key aspects of the study as highlighted at the beginning of the chapter. The most relevant literature in the key areas of the study, which are financial crimes, financial crime in organisations, technology adoption and detective analytics were highlighted. The review is conducted in an interrelated manner, enabling logical flows. Through the logical flow of the literature review, some of the gaps in the phenomenon being studied were identified. The next chapter discusses the theoretical framework used as a lens to underpin the study.

CHAPTER THREE
THEORETICAL FRAMEWORK

3.1. Introduction

This chapter presents a review of the theoretical frameworks used to underpin the study. The review is based on the objectives of the study as stated in Chapter One. This means that the review focuses on how the two theories actor-network theory (ANT) and the activity theory (AT) are used as a lens to guide the data analysis and the interpretation of findings of financial crimes in organisations. Thereafter, a theoretical framework is developed to show how ANT and AT will be used to complement each other to achieve the study's objectives.

The remainder of this chapter is structured into four main sections. The first section focuses on providing an overview of the underpinning theories. In the second and third sections, the actor-network theory and activity theory are discussed. In the fourth section, the theoretical framework is developed. The application of the theoretical framework is discussed in section five. Finally, the chapter is summarised in the last section.

3.2. Overview of the underpinning theories

This study is underpinned by two socio-technical theories, ANT and AT considering the objective of the study is to understand the nature of financial crimes that happen in South African financial institutions and to examine the current preventative and mitigative measures. The two socio-technical theories are selected based on their strength to understand which role human and non-human actors play in the identified problem, the rules followed and the tools used (Nehemia-Maletzky et al., 2018). ANT aids the process of understanding the negotiations that occur during the financial activities which happen between humans and the technologies involved. Iyamu (2021) stated that the primary objective of using ANT is to unpack the actors, network, and translation. Callon (1986) alluded that another critical focus of ANT is to understand the negotiation shifts among actors, consciously or unconsciously.

AT is used to interpret the findings based on the data analysis conducted by applying ANT as a lens to guide the process. AT will guide the interpretation of findings to understand the activities of humans in conducting these financial crime activities in their use of tools. Nardi (1996) states that from the AT perspective, the relationship is discovered through its components, which are tools, subject, rules, community, division of labour, and the object, which is the outcome. AT will be used to interpret the findings and understand which findings are associated with tools used to commit these financial crimes, the subjects involved, the rules being followed and not being adhered to, the community in which these financial crimes happen and affect, and the division of labour based on different opinions of these financial crimes. Without a complementary use of the ANT and AT, there would be a gap, either in analysing the data or interpreting the findings. Iyamu (2021) provides a comprehensive justification and offers a guide for employing AT and ANT complementarily.

3.3. Actor-network theory

The Actor-network theory (ANT) is a sociotechnical theory that is used by researchers to explain the relationship between humans and non-human objects (Couldry, 2008). Crawford (2020) describes ANT as a methodology used in the sociology of science and technology that defines the activities of the social system of actors (human and non-human). The first objective of the study is to understand the nature of financial crimes that happen in South African financial institutions. The nature of the study requires a socio-technical view. The ANT will aid the focus on fraudulent financial activities, and negotiations that occur between humans, technologies, or humans and technology actors.

An actor network is formed immediately when actors have found a common ground which can occur consciously or unconsciously (Latour, 2007). There are many networks formed by perpetrators conducting financial crimes, using technology to access and manipulate the data or the technologies used to process financial transactions. The actor network focuses on how networks are built and maintained and what makes the network dissolve (Shim & Shin, 2016). The main objective is to understand the nature of financial crimes that happen in South African financial institutions and, thereafter, examine the current preventative and mitigative measures. To understand the nature of these financial crimes the actors have to be followed, enabling the tracing and tracking of the time the crime occurred and how it occurred.

These financial crimes would have to be traced and translated to understand the specified occurrence. In ANT, translation is the process that allows a network to be represented by a single entity, which can in itself be an individual or another network. Callon's ANT model of translation comprises four moments or phases shown in Figure 3.1: problematisation; interessement, enrolment, and mobilisation. During the first phase, problematisation, the primary actor attempts to identify the problem, the knowledge claim required, and what actors are required within the network. The second phase is interessement, which is when an actant (or more) attempts to impose and stabilise the identity of the other actors. Negotiation leads to enrolment; actors accept the roles they have been given and enrol in the network. Mobilisation then occurs as others external to the network (allies) move to support it.

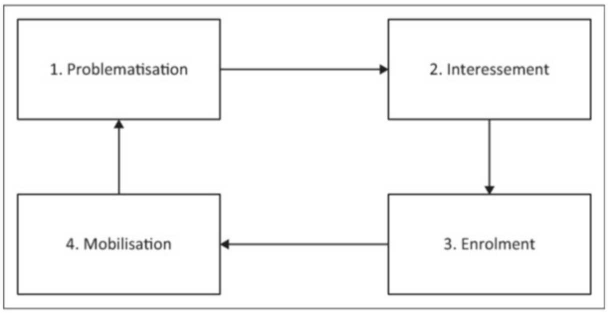

Figure 3.2: Four moments of translation (Callon, 1986)

Tables 3.1 and 3.2 below critique the use of ANT for this study and justify why the sociotechnical theory strength impacts the study.

Table 1.1: Weaknesses of ANT

Weaknesses of ANT	How the weaknesses impact the study
Limited analysis of social structures to understand how actors interact and work together (Dolwick, 2009).	The actors involved in committing financial crimes are both human and non-human; however, ANT has no social structure to understand their relationship.
The theory's stance on moral and political issues within the network (Sayes, 2014).	The inclusivity of both human and non-human actors makes it hard to understand the morals and political issues of the actors, especially of non-humans.
The equality of treatment between human and non-human actors (Bueger & Stockbruegger, 2017).	The actors within the actor network can be equal; however, their treatment will not be the same.
The ability to describe and not explain (Latour, 2017).	The ANT moments of translation tenet provides details of the process of translation but not how it should be understood.

Table 2.2: Strengths of ANT

Weaknesses of ANT	How the weaknesses impact the study
The power relationship to understand the relationship between humans and non-humans (Crawford, 2020).	Financial crimes are committed by humans through the use of non-humans. The power relationship will help to understand the nature of these crimes.
The stability of the network, to understand how a network between humans and non-humans is formed (Steen et al., 2006).	To understand the nature of these financial crimes the actors have to be followed, enabling the tracing and tracking of the time the crime occurred and how it occurred.
The negotiation scheme of understanding negotiation shifts among actors, consciously or unconsciously (Iyamu, 2021).	To understand how the shift in negotiation among actors happens to get to the point of committing these financial crimes.
All actors are equal, whether human or non-human (Kolli & Khajeheian, 2020).	With the power of technology being used to store and process financial transactions, human actors cannot commit financial crimes without non-human actors.

3.4. Activity theory

The AT was designed formally by Leont’ev in the 1920s and 1930s and further developed by Engestrom in 1987 with its primary role being to evaluate activity systems with its objects and subject actions (Wells, 2002). AT, according to Iyamu (2021), has been applied in studies over 3 million times. The theory is primarily applied in Information systems (IS)/Information technology (IT) studies to understand and evaluate the use of technologies within organisations (Kaptelinin & Nardi, 2018). The AT provides a lens for studies to understand the design of certain processes, rules, and tools used to achieve an outcome (Futerman, 2015). Due to the nature of qualitative studies, understanding the relationship between actors and activities can be subjective and unstructured. Therefore, AT provides a framework that guides the process of understanding the relationship and human activity (Iyamu, 2020).

The AT is used as a lens for this study to examine and understand the relationship between the human mind and financial crime activities. Sukirman and Kabilan, (2023) aver that AT serves as an analytical tool that can aid studies to understand people's actions and what leads to their actions to analyse their behaviours. This will assist the investigation of how the detective analytics tool can be deployed, to trace, track, and prevent financial crime in a financial institution. The technology role in information systems is hardly assessed according to the role that humans play in it. AT provides a lens to understand the relationship between actors and their tools which could be software or hardware (Karanasios & Allen, 2018; Kaptelinin & Nardi, 2018).

The theory consists of a model commonly applied in IS/IT studies. It is referred to as the AT model, shown in Figure 3.2. In AT, the unit of analysis used is the activity in which there is an interaction between the subject and object using tools to accomplish a desired outcome (Carvalho, 2015). The activities in AT can be internal or external and for this study, there is a need to understand both internal and external financial crimes that affect and impact financial institutions (Kirby & Anwar, 2020). As shown in Figure 3.2, from the perspective of AT, the relationship is discovered through its components which are tools, subject, rules, community, division of labour, and the object which is the outcome (Nardi, 1996).

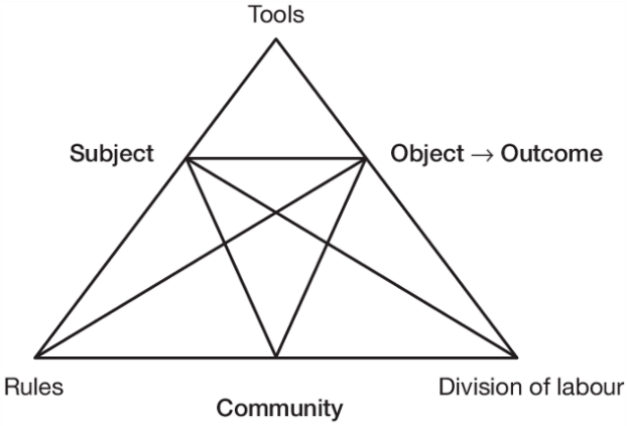

Figure 3.2: Four moments of translation (Callon, 1986)

The tools used to commit financial crimes can be hardware or software (Bertelsen & Bødker, 2003). Iyamu (2020) defines a subject as a living being. There are rules defined in all processes and in AT this is translated through the conditions and laws associated with the activity (Tessier

& Zahedi, 2022). The community within the activity system plays a huge role in understanding the relevant actors based on the cultural rules and how the community perceives something (Karanasios, 2014). In AT, the community comprises the participants within the activity (Murphy & Rodriguez-Manzanares, 2008). The division of labour within the activity is created due to different opinions which arise based on contradictions and conflicts within the workplace (Avis, 2009). The division of labour is also associated with the power dynamics and status of the actors within the community (Murphy & Rodriguez-Manzanares, 2008).

Tables 3.3 and 3.4 below critique the use of AT for this study and also justify why the socio-technical theories' strength impacts the study.

Table 3.3: Weaknesses of AT

Weaknesses of AT	How the weaknesses impact the study
Lack of standardised methods for its application (Bertelsen & Bødker, 2003).	The application of the AT as the lens to guide data analysis is not standardised; therefore, the use is subjective.
Lacks consideration of other factors that may influence the relationship between activity and the subjects (Bedny et al., 2000).	Some financial crime perpetrators are influenced by their surroundings and the community that they reside in or based on their upbringing.
Complete understanding of the activity system (Collins et al., 2002).	The activity system needs to be well understood for the study to understand the nature of financial crimes that happen in South African financial institutions.
Insufficient methods and techniques to solve problems (Raeithel, 1992).	The AT is not enough to understand human activity and for this study to understand and solve the occurrence of financial crimes.

Table 4.4: Strengths of AT

Weaknesses of ANT	How the weaknesses impact the study
The AT bridges the gap between the individual subject and the social reality (Engeström, 1999).	To understand the nature of financial crimes that are committed by perpetrators and how the social reality impacts these crimes.
The emphasis is on the community role (Engestrom, 2000).	The theory recognises the role of the social community in shaping criminal behaviour, which can help inform crime prevention and reduction efforts by using a detective analytics instrumentation.
Understanding the rational capabilities of an individual (Kaptelinin & Nardi, 2009).	The AT enables ease of understanding of how individuals use technology and the intended purpose of committing financial crimes.
Offering a comprehensive understanding of the social context in which technologies are used (Engeström et al., 1999).	To understand the social context of these financial crimes and the technologies, as well as point out conflicts and interactions between perpetrators and activity components.

3.5. Theoretical framework

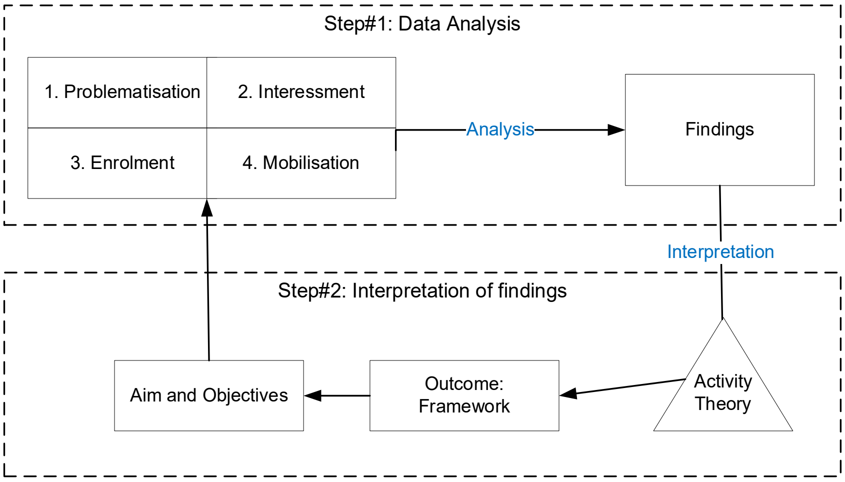

Figure 3.4: Order of use

The framework as shown in Figure 3.3 is developed to guide the use of the two theories ANT and AT. This figure illustrates the order in which the two theories will be used for the study. ANT is used as a lens to guide the data analysis and the findings are interpreted using AT. The main component of the framework includes ANT's moments of translation, findings, the activity system, output or framework and the research aim and objectives. To achieve the research objectives, these theories' components are interconnected and dependent on each other. The framework is applied as a lens for data analysis and interpretation of findings as follows:

1. Step 1: The four moments of translation, namely, problematisation, Interessement, enrolment and mobilisation were used to guide the data analysis. Based on the data analysis conducted, findings were noted and listed for interpretation.
2. Step 2: The interpretation of findings was conducted and guided by using AT as a lens. Based on the interpretation of findings, an outcome was achieved which is the instrumentation; a tool/framework that can be used to implement detective analytics to mitigate financial crimes. This, therefore, achieves the aim and objectives of the study.

3.6. How it is applied in the study

3.6.1. Actor-Network theory in information systems

ANT in the IS/IT domain has been used by researchers to explore the role of human interactions with technology (Alexander & Silvis, 2014). Doolin and Lowe (2002) state that using ANT in IS/IT aids the understanding of heterogeneous networks that are formed when adopting or using technologies. The strength that ANT brings to information systems is the ability to understand how people interact with technology (Tatnall, 2003). Sage et al. (2020)

explored how organisations adopt new technologies using the theory as a lens to guide their study. Klecuń (2004) implies that studies often use ANT for IS research due to its complex capability of conducting empirical studies.

3.6.2. Activity theory in information systems

AT is used in IS/IT to understand the overall activity system before an outcome is reached (Collins et al., 2002). Multiple decisions are taken in IS that ensure that systems are operating as intended and that there is continuous monitoring for oversight of the operation. The use of AT allows IS studies to understand the relationship discovered through its components; tools, subject, rules, community, division of labour and the object which is the outcome (Nardi, 1996).

3.7. Summary

The purpose of the theoretical framework chapter was to outline the order both ANT and AT followed to get an in-depth understanding of the nature of financial crimes that happen in South African financial institutions. Nehemia-Maletzky et al. (2018) provide a guide for the complementary use of both AT and ANT in IS studies. ANT and AT were complementarily used in this study to conduct the data analysis and interpretation of the findings.

CHAPTER FOUR
RESEARCH METHODOLOGY

4.1. Introduction

The Research Methodology chapter presents the methods followed to conduct this study. A research methodology is defined as the different techniques and methods used to conduct a study (Chivanga & Monyai, 2021). This chapter details the systematic approach used to investigate the research questions posed to achieve the research objectives. The chapter provides a comprehensive explanation of the methods and procedures adopted to ensure the validity, reliability, and accuracy of the research. The study is qualitative and conducted through an interpretivist approach to understanding financial crimes.

The remainder of this chapter is structured into seven main sections. In the first section, the philosophical assumption is provided. This is followed by the research approach in the second section. Thirdly, the research method is outlined. Fourth is the research design section. The data collection process is listed in the fifth section, followed by the data analysis process in the sixth section. Finally, the unit of analysis is covered and the chapter is summarised.

4.2. Philosophical assumption

Philosophical assumptions are defined as the beliefs and different perspectives of conducting research (Sibanda, 2022). Three philosophical assumptions are known in information systems research which are ontology, epistemology and axiology (Setiawan & Syamsuddin, 2022). Ontology is defined as the reality of the existence of the phenomena; epistemology is on the knowledge of the phenomena and axiology is on the values and principles of the phenomena (Yulianto, 2021; Hayati & Dalimunthe, 2022). The philosophical assumptions, therefore, focus on the reality of existence, knowledge and values of the phenomena.

Three assumptions exist based on the stance taken for any research, namely; interpretivism, positivism and pragmatism (Faried, 2018). Interpretivism is defined as an assumption that the reality of phenomena is subjective and is socially constructed (Baloyi, 2020). Positivism is defined as a scientific study to prove a specific outcome to be either true or false (Monteiro & Kahlke, 2022); and pragmatism is defined as solving a problem by being practical and not by using theory (Clarke, 2021). An interpretivist stance is taken for this study as it allows for the understanding of financial crimes that are currently happening and to understand the tools currently in use to detect them.

Ontologically, there are many realities to how financial crimes happen and are detected in financial institutions. Detective analytics is viewed and understood from different perspectives based on different events and usefulness. Islam et al. (2021) stated that detective analytics was used for their research to discover suspicious behaviour of life insurance policy owners. Detective analytics is not only used in the financial sector. Yaqot and Menezes (2021) state that detective analytics can also be used to monitor the agriculture sector by using data obtained through drones to detect any anomalies in day-to-day activities. The study will influence how to implement detective analytics to mitigate financial crimes, through an instrumentation.

Epistemologically, different financial crimes occur and are known to affect individuals and organisations both internally and externally. However, financial institutions do not seem to have a tool that detects these financial crimes as and when they happen. The objective of the study is to first understand the types of financial crimes that happen internally and externally, and thereafter, investigate how the detective analytics tool can be deployed to trace, track, and prevent financial crime in a financial institution.

4.3. Research approach

A research approach is defined as the viewpoint that the study will undertake to learn and discover new things about the phenomena (Behfar & Okhusen, 2018). Three research approaches exist in research, namely, deductive, (Hellstrand & Breckwoldt, 2016), inductive, and abductive (Buqa & Fung, 2019). The deductive approach assumes that there can only be one answer to the problem and the answer can either be true or false (Mitchell & Education, 2018). Deductive reasoning is mostly applied in quantitative studies where the study wants to test a specific hypothesis for an outcome that can either be true or false without any debates (Ganesan et al., 2019). Whereas, the inductive approach is applied in studies where the answer can never be a simple yes or no but rather requires logical thinking to understand the patterns within the data (Behfar & Okhusen, 2018).

The inductive approach is used in qualitative studies to gain more knowledge about the phenomena and to create themes and patterns of the data collected (Azungah, 2018). Lastly, the abductive research approach is a combination of inductive and deductive research approaches which is used in a phenomenon where the research method is mixed (Osman et al., 2018). The inductive approach was followed based on the aim and objectives of the study. The approach allows the researcher to induce his/her reasoning into the field of study and find solutions to a problem (Thomas, 2006). Inductive reasoning allows the study to make observations on the phenomena to create a research hypothesis (Bryman, 2016). The inductive approach is applied mostly in information systems studies to understand different viewpoints of the phenomena being studied. The main objective of the study is to understand the nature of financial crimes that happen in South African financial institutions and, thereafter; examine the current preventative and mitigative measures.

Based on the study's aim, which is to develop an instrument that can be used for mitigating financial crime within the financial institutions in the South African context, the inductive approach is deemed appropriate for the study. Two theories, AT and ANT, were therefore used in the study to understand the fraudulent financial activities and negotiations that occur between humans, technologies, or humans and technology actors.

4.4. Research method

There are two commonly used research methods in information systems studies, namely, quantitative and qualitative methods (Apuke, 2017; Gerring, 2017). Some studies apply the combination of qualitative and quantitative, which is referred to as the mixed method (McCusker & Gunaydin, 2015). Quantitative research is focused on the numerical representation of the data by using statistical tools or graphical totals (Scharrer & Ramasubramanian, 2021), whereas the qualitative research method is focused on understanding and observing the phenomena based on the interaction with the data collected (Bazen, Barg & Takeshita, 2021). The aim and objectives of a study determine which research approach is appropriate. The research approach chosen for this study is qualitative. It was deemed appropriate as it allows us to describe and understand the nature of the financial crimes happening in financial institutions in the South African context.

The qualitative research method is the most preferred in information systems research as it allows the study to establish a relationship between technology and the social aspects of its use by humans and non-humans (Lee & Liebenau, 1997). Nguyen et al. (2021) argue that due to its subjective nature, the qualitative research method allows the researcher to vocalise their judgement on the study. Fossey et al. (2002) explain that understanding the experience and meaning of people's lives and social environments is one of the main goals of qualitative research. The study seeks to understand the nature of financial crimes that happen in South African financial institutions; therefore, qualitative research methods allow the study to establish the relationship between financial crimes and the instrument that is developed to define and enable the implementation and use of detective analytics to mitigate financial crimes.

Financial crimes happen in almost all organisations across the globe; however, due to their complexity and different natures, their perspectives may vary. To understand these crimes, the researcher needs to apply their subjectivism and interpret them in a way that makes it easy to express using natural language. This was done through collecting data using qualitative interviews which the study had to understand and narrate based on the understanding of what was being said about the occurrence and nature of financial crimes within the organisations.

4.5. Research design

A research design is defined as the technique or method used for collecting data to answer the research problem and questions (Rezigalla, 2020). Qualitative research has multiple research designs such as ethnography, phenomenology, grounded theory, action research and case study (Chapter, 2004).

Ethnography research involves the study of people in their cultural setting, which includes immersing oneself in the cultural setting of the people being studied to gain a deep understanding of their daily lives, practices, and beliefs (Simanjuntak & Hendriani, 2022). Phenomenology focuses on the first-hand human experience, exploring and understanding how a phenomenon comes to being (Lundh, 2020). Grounded theory research design focuses on generating or discovering theories or a hypothesis through data collection and analysis (Dunn et al., 2023). Action research is a participatory research design that studies an individual's actions and their effect on an organisation (Hoa, 2024). These research designs were not suitable for the study as they focused on people and cultural settings.

For this study, the case study approach and documentation of existing materials was used. A case study approach is defined as a thorough investigation into an individual, a group of individuals, or a business unit to generalise over similar setups (Mfinanga et al., 2019). A case study is appropriate for this study as it allows for an understanding of the nature of financial crimes that happen in South African financial institutions and, thereafter; examining the current preventative and mitigative measures. The case study research design is valuable for exploratory research, helping to develop and refine theories, frameworks and models based on empirical evidence (Ebneyamini & Sadeghi Moghadam, 2018). Case studies allow researchers to delve deeply into a phenomenon that is difficult to capture through other research designs; this is especially useful when the goal is to understand the intricacies of a phenomenon (Ridder, 2017).

One organisation was selected as a case for this study. Existing documents were collected to ensure rigour in understanding the nature of financial crimes that happen in South African financial institutions. Before the organisation was selected for the study, an investigation was done based on understanding if the organisation had adopted detective analytics or was planning on adopting the tool. A set of criteria were formulated and used to select the organisation. The set of criteria included: (i) the organisation must be aware of detective analytics; (ii) the organisation must be willing to voluntarily participate in the study; and (iii) the organisation must be based in the province in which the researcher lives, for proximity purposes.

The organisation selected as a case for this study is one of the South African major financial institutions. The identity of the organisation is kept anonymous; therefore, a pseudo name Nikiwe Federal Finance (NFF) is assigned to the organisation. For this study, the organisation selected should be knowledgeable about detective analytics and be willing to participate. The selected organisation was based in the same province as the researcher. A list of organisations within the province that might meet the criteria was created. This was done through business directories, industry associations and local networks. Formal inquiries were sent to the organisations explaining the study and requesting their participation, including details about the study, objectives, methods, and benefits to the organisation. The selected organisation therefore met the criteria and the necessary documentation, such as consent forms and data collection instruments was completed for data collection. Participants were allocated for the researcher to schedule meetings, interviews, or data collection sessions.

4.6. Data collection

Data collection is defined as the process of gathering data to achieve the aim of the study (Mazhar et al., 2021). Sukmawati (2023) states that the process of data collection Is done in studies to search for information regarding the investigation being carried out on the phenomena. There are many data collection methods for qualitative studies such as questionnaires, observations, focus groups, grounded theory and interviews (Gupta, 2024). Data for this study was collected through interviews; however, Dubovsky (2024) states that there are three different types of interviews, namely, unstructured, structured and semi-structured. An unstructured interview is conducted through the freestyle approach where the interview questions are not formulated beforehand (Chauhan, 2022). A structured interview is carried out in a manner where there are set questions which are to be answered with either yes or no or true or false (Young et al., 2018).

This study collected qualitative data through conducting semi-structured interviews within the selected case. Semi-structured interviews are defined as the ability to have both closed and open-ended questions which allows the interviewer to probe based on answers for each question (Adhabi & Anozie, 2017). The semi-structured interview technique is deemed suitable for this qualitative study as it allows for an in-depth investigation between the interviewer and interviewees to understand the nature of financial crimes that happen in South African financial institutions. Adeoye-Olatunde and Olenik (2021) affirm that semi-structured interviews allow the researcher to have a format of questions to guide the flow of the conversation for ease of continuation. The interview questions (guidelines) were extracted from the research questions.

The interviews were conducted one-on-one with the participants at their preferred locations. The interview sessions were recorded using Microsoft Teams. From the participants, the researcher requested permission to record the interview process. The data collected is stored in the institutions' access-controlled data management system. The CPUT data management plan was completed and used to manage data collected for the study.

A total of 12 participants participated in the study. Six (6) of the 12 participants were employed in the business department and the other 6 were employed in the information technology (IT) department. A set of criteria were used in selecting the participants. The criteria are presented and discussed in section 4.6.1, below. A point of saturation was reached at 12 participants. In qualitative studies, a point of saturation is defined as the point or extremity where the researcher obtains the same information from the participants (Moser & Korstjens, 2018).

A total of 40 papers were collected from database sources such as AIS, EBSCOhost, Gartner, IEEE, and Emerald. There were two keywords used to search for these papers which were detective analytics and financial crime. The two keywords were deemed appropriate as they narrowed the search on the databases to the context on which this study focuses. 26 of the 40 papers were focused on detective analytics and 14 of the 40 papers were on financial crimes. The sources were important because they instilled credibility and reliability in the data (Nyikana & Iyamu, 2023).

4.6.1. Criteria for selecting participants

Selecting participants for research is a critical step. This is because it significantly impacts the validity and reliability, including the richness of the data (Subedi, 2021). The criteria ensure that participants understand the research objectives and questions. This helps in gathering relevant data, within the context that directly addresses the research objectives and aim (Northcote, 2012). Thus, a set of criteria was formulated for the selection of participants for the study. The criteria include, that the employee must (i) be employed in the finance or IT department or division of the organisation; (ii) have experience with financial crime in the organisation; (iii) know about detective analytics; or (iv) be part of the unit or department that provides, supports or manages solutions for mitigating financial crimes in the organisation.

4.6.2. Ethics implication

Ethical considerations in qualitative research are crucial. Ethics helps to ensure that the study respects participants' rights, and the organisation's rules, maintains integrity, and produces reliable and valid results (Taquette & Borges da Matta Souza, 2022). Cape Peninsula University of Technology (CPUT) has an ethics procedure which must be followed to guide the process of data collection. This study adheres to CPUT's research ethics. To proceed with data collection the research received ethical clearance from the university and an agreement from the case being used.

The case being studied also has ethics that must be considered and adhered to. This includes a rigorous process. Firstly, an ethical form must be completed by the researcher and submitted to the organisation for review and approval. The form must be signed by both the researcher and the supervisor. Due to the nature and sensitivity of the data collection regarding financial crimes and its jurisdiction in a financial institution, there were legal requirements that mandate the protection of confidentiality for both the organisation and the university. Secondly, a confidentiality agreement was signed between the researcher, supervisor and the organisation. This agreement had to be completed to build trust among participants and stakeholders (University, NFF and the researcher), ensuring comfort in providing honest and accurate information. Thirdly, the organisation's legal department had to ensure that the agreement was signed and agreed by all stakeholders to keep the anonymity of NFF and the participants before the researcher was allowed to commence the study. The departmental heads, university and researcher's agreement reinforces the organisation's commitment to these ethical standards.

The study adhered to the ethics by ensuring that there was no potential for harm; physical, psychological, social, cultural, or financial, to participants. The research did not involve any substance, procedure, or methods that directly or indirectly harmed the environment. The participants were recruited to take part in this research and none of the participants felt coerced to participate. There was no dependent relationship between the investigator and any of the participants. None of the participants were offered an inducement to encourage their involvement and all of them participated voluntarily. When the study was introduced to them, those who wanted to participate agreed by accepting the interview invitations. No participants were deceived by the researcher. Moreover, written consent was obtained from the participants. There is no possibility of participants being inadvertently identified or confidential data being divulged during or after the research. Lastly, no conflict of interest including financial gain resulted from this project.

4.7. Data analysis

Analysing data entails examining, eliminating unnecessary information, and translating it into the patterns and themes that identify and formulate your findings (Selvan & Balasundaram, 2021). Data collected through semi-structured interviews were cleaned and coded which Harwalkar et al. (2023) describe as the process of fixing or eliminating inaccurate, redundant, or incomplete data that exists inside the dataset. The coding of the data entails that each participant's interview be coded differently and each participant be given a pseudonym to ensure anonymity. The collected data was therefore ready to be used in the data analysis section through translation. The thematic technique was employed in the analysis. Complementarily, the analysis was guided using ANT as a lens for the data analysis. ANT is discussed in detail in the theoretical framework in Chapter 3.

ANT was used to understand how networks of actors are consciously or unconsciously formed. This allowed actors to be followed to establish their roles in the processes and activities in finance transactions within the organisation. ANT helped in gaining insights into how negotiation shifts among actors during finance transactions within the organisation. ANT was used to gain a deeper understanding of the relationship that exists between the actors in the process of executing financial transactions. This includes committing a financial crime or attempting to mitigate the financial crime.

4.8. Unit of analysis

A unit of analysis is based on who or what is being analysed for the study. The data was split into two units for analysis purposes. The units were IT and business departments within the organisation. Also, the business and IT department units were further split into levels, as shown in Table 4.1. This was to gain deeper insights, firstly, from both technical (IT) and non-technical (business) perspectives, and secondly, to comprehend experiences and perceptions from employees at different levels of the organisational structure.

Table 5.1: The units of analysis

Department	Unit
IT department	Business solutions team
	Data analysts' team
	IT security
	Machine learning team
Business department	Compliance and enforcement
	Financial surveillance
	Risk management
	Prudential authority
	Money laundering

The units helped since many actors were involved in detecting and preventing financial crimes in the organisation. Also, ontologically, there were many realities concerning how, why, and when financial crimes happen in the organisation. Data was collected at different levels. At the time of this study, financial crimes were experienced by many users in the organisation, from IT individuals who were involved in developing solutions and implementing processes to business individuals who were involved in the planning and monitoring of processes.

4.9. Conclusion

The purpose of the research methodology chapter was to outline the methodology followed to get an in-depth understanding of the nature of financial crimes that happen in South African financial institutions. This qualitative research made use of inductive reasoning to observe and create patterns, applying an interpretivist viewpoint to investigate how the detective analytics tool can be deployed to trace, track, and prevent financial crime in a financial institution. Data was collected, using semi-structured interviews and existing documentation. ANT was used as a lens to guide the data analysis.

CHAPTER FIVE
OVERVIEW OF DATA COLLECTION

5.1. Introduction

As discussed in Chapters 1 and 4, the study used the case study approach and documentation in its design. This means that an organisation that met the criteria to participate in the study was used as a case. Subsequently, data was collected from the organisation. Existing material was collected using the document analysis technique. This chapter presents an overview of the case, the organisation that was selected for this study and the documentation that was collected and used. It is important to provide useful information about the organisation and how the data was collected. However, the identity of the organisation was kept anonymous. Therefore, a pseudo name, Nikiwe Federal Finance (NFF), is assigned to the organisation. Furthermore, the chapter presents the types of documents that were collected.

This chapter is divided into three main sections. In the first section, an overview of the sources of data is presented. This is followed by the fieldwork conducted. In addition to the information about the organisation, the chapter provides a discussion on how the fieldwork was conducted in the organisation. Next is how the existing data was collected and the credible sources used. Finally, the chapter is summarised in the last section.

5.2. Overview of data sources

This section provides categorises the origins from which data was collected for this study for better understanding. Two data sources were used to collect data and are referred to as primary and secondary data. Primary data is defined as the data collected for the first time through interviews, questionnaires or direct observation at first hand by the researcher (Sandhya & Sujitha, 2022). Taherdoost (2021) defines secondary data as data obtained from existing materials. The primary data for this study was obtained through conducting semi-structured interviews at NFF. The secondary data was collected through a literature survey using a document analysis technique which is explained in detail below.

5.3. The organisation: Nikiwe Federal Finance

The organisation from which the data was collected is NFF, which is one of South Africa's major financial institutions. The organisation was formed just over a century ago and as of the time of this study, the organisation had between 1000-5000 employees, including contract and permanent employees. The selected organisation is a diversified African financial institution which provides services in many countries such as Belgium, Japan, Greece, Italy, Türkiye, Switzerland, South Africa, and the United States. The organisation also has over two million issued shares of which, by policy, no one individual may own more than ten thousand shares.

The headquarters of the organisation are in Johannesburg and this study was conducted in the headquarters in South Africa. The organisation is structured into 2 departments, namely, business and IT.

5.3.1. Business department

The business department plays a crucial role in preventing and mitigating financial crimes within the organisation. The department consists of over 300 employees. As shown in Figure 5.1, the business department comprises 5 units which were the focus of this study. The units were compliance and enforcement, financial surveillance, risk management, prudential authority, and money laundering. Each of the units had a head. For example, the chief financial officer (CFO) oversees the business department, particularly financial management, compliance, and risk assessment. The chief compliance officer (CCO) ensures that the department adheres to legal and regulatory standards.

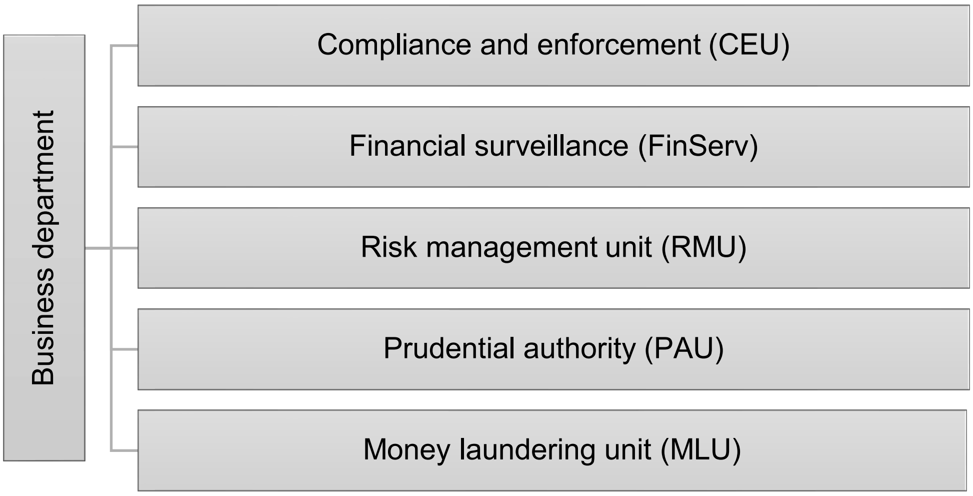
Business department
Compliance and enforcement (CEU)
Financial surveillance (FinServ)
Risk management unit (RMU)
Prudential authority (PAU)
Money laundering unit (MLU)

Figure 5.5: Business department structure

The senior managers and heads of different units oversee the business department's day-to-day operations and strategic initiatives. Within the executives sits the audit committee which is responsible for overseeing accuracy in financial reporting and internal standards controls. The internal auditors review the department's processes and controls to ensure there are measures and controls for preventing and mitigating financial crimes. The compliance and risk management team is just as crucial as the audit to oversee factors contributing to financial crime prevention and mitigation, ensuring that the department adheres to best practices and regulatory requirements.

5.3.1.1. Business units

Each of the business units, the compliance and enforcement unit (CEU), financial surveillance (FinServ), risk management unit (RMU), prudential authority (PAU), and the money laundering unit (MLU) had about 50 employees at the time of this study. Also, each unit had distinctive deliverables. However, there was collaboration between the units in carrying out their distinctive tasks.

The role of the CEU unit is to facilitate the organisation's risk management, specialised operational risks, and compliance management, and provide advisory services to other departments in the organisation based on their risk appetite. Based on the unit’s role, each of its employees was tasked with minimising risk exposures, governance, compliance and risk management. Additionally, the CEU was mandated to ensure that NFF adheres to legal, regulatory, and internal standards. In fulfilling its mandate, the unit focuses on preventing, detecting, and addressing non-compliance and enforcing relevant laws and regulations concerning the prevention and detection of financial crimes.

Similar to the CEU, tasks were allocated to individuals. Each employee in the Financial Surveillance (FinServe) unit was assigned the responsibility of detecting and mitigating financial crimes on behalf of the organisation. Within the FinServ team, there were specialists dedicated to applying data analytics to provide reporting of all transactions performed by authorised dealers with limited authorities such as Mukuru, Mpesa, and Mama Money, including other commercial banks in the country. The NFF financial crimes capabilities could not be a success without the FinServ employees who were responsible for the daily administration of exchange controls in South Africa.

The risk management unit (RMU) focuses on the identification, prevention, and management of risk on behalf of the organisation. Thus, the employees were responsible for identifying, assessing, and mitigating risks that could potentially impact NFF's financial operations, financial health, and strategic objectives. Risk identification is the process of outlining potential risks that could affect NFF, including financial, operational, strategic, compliance, and reputational risks. The risk assessment involves the evaluation, likelihood and potential impact of any identified financial crime risks. This includes the application of categories to assess the severity and probability of the financial crimes’ occurrence. The risk mitigation aspect ensures that strategies and controls are developed to mitigate identified financial crime risks. This also ensures that weekly risk reports are prepared for senior management and the stakeholders to highlight any key risk issues and trends.

The Prudential Authority Unit (PAU) is responsible for overseeing and ensuring the stability, safety, and soundness of NFF and its financial markets. The primary role of PAU is to maintain financial stability and protect depositors, policyholders, and other stakeholders by enforcing prudential standards. The employees are responsible for maintaining financial stability on behalf of the organisation including collaborating with regulators and other stakeholders. The unit has layers of roles and responsibilities. The primary role of the PAU is to supervise all financial institutions that provide products and services to support financial inclusion. Furthermore, the PAU monitors and assesses risks within the financial sector, including credit risk, market risk, operational risk, and systemic risk. The PAU's secondary responsibility is to the organisations' customers' interests by ensuring that NFF operates with transparency and fairness.

The employees in MLU have a mandate to detect, prevent, mitigate, trace, track and monitor money laundering activities within NFF. This unit is responsible for implementing and overseeing measures designed to prevent illicit financial activities and ensure compliance with anti-money laundering (AML) regulations. The MLU also implements processes for customer identification and verification to assess the risk profile of clients. The prior vetting is to know their customers. Furthermore, MLU has adopted automated systems and data analytics that detect unusual patterns and anomalies in the transaction data to warrant further investigation. The MLU performs investigations daily and reports suspicious activities to the relevant stakeholders.

5.3.2. IT department

The IT department is divided into four (4) units, which are business solutions, data analysts, IT security, and machine learning, as shown in Figure 5.2. Data for this study were collected from the four units, as explained in Chapter 4. The IT department's primary role and mission is to provide IT business solutions to the organisation and IT support. The IT department consists of over 200 employees. The chief information officer is the head of the department and has the chief technology officer who oversees the different divisional heads and their respective reporting lines and employees.

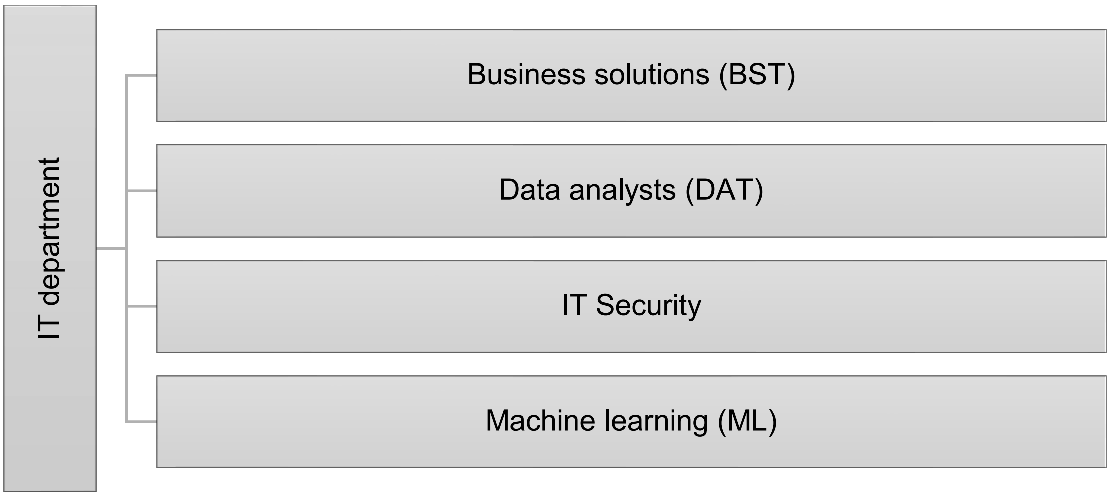

Figure 6.2: IT department structure

Each of these 200 employees is responsible for the organisation’s enterprise architecture, project management and development, internal business support for applications and systems, IT strategy, and stakeholder relationship management. The primary role of the department is to ensure that all transaction data is secure, all applications and systems used in the organisation are safe, and no unauthorised individuals may access the data, systems and the organisation's applications. The IT department is very critical because of its role in ensuring business continuity for all daily operations as the organisation works and relies more on technologically enabled business operations.

5.3.2.1. Information Technology units

The business solutions team (BST), data analysts’ team (DAT), IT security, and machine learning team (MLT) have over fifty (50) employees each. Each unit of the IT department has its deliverables. Collectively, the units enable and support the organisation’s processes and activities.

The BST is responsible for creating harmony between business needs and technology solutions. The BST’s primary role is to continually understand the requirements of different business units regarding their financial crime operations. This is to be able to provide IT solutions that enhance operational efficiency, support business objectives, and drive digital transformation. The BST manages IT projects from initiation to completion, including defining project scope, timelines, resources and overall IT project management. Moreover, the BST creates and maintains documentation for IT solutions, including user manuals, system specifications, and project reports.

In the context of financial crimes, the DAT plays an important role in identifying, preventing, mitigating and investigating financial crimes through the effective use of data. The unit's primary responsibilities entail analysing and interpreting a variety and veracity of data to uncover patterns, detect anomalies, and provide insights that support business decisions and investigations. The DAT specialists also have skills that can gather and integrate data from various sources, including transaction data records, customer information, and external data feeds from other financial institutions. The team uses large volumes of financial data and machine learning techniques to detect anomalies and outliers that could suggest financial crimes such as money laundering, fraud, or insider trading.

The IT Security Team plays a critical role in protecting the organisation's information systems, applications and data from cyber threats and unauthorised access. Their responsibilities are focused on ensuring the security and integrity of IT infrastructure, which is essential for detecting, preventing, and investigating financial crimes. The team monitors and analyses network traffic, system logs, and other data to detect and respond to potential cybersecurity threats, including hacking attempts and malware infections. Furthermore, the team implements and enforces access controls, including creating a virtual private network, authentication, and authorisation mechanisms, to ensure that only authorised personnel can access sensitive information and systems. The data were collected from the IT and business departments, and fraud and financial crime specialists.

The machine learning team is responsible for creating automated solutions that can learn and determine patterns using the transaction data. Their responsibilities are focused on creating machine learning models using artificial intelligence and training these models using technologies such as robotic process automation (RPA), detection models and interactive agents such as chatbots. The team monitors and maintains these models to ensure that they are operating as intended. Furthermore, the team develops, trains and implements these models throughout the organisation for both IT and business departments. This ensures that they have an overview of all transaction data being generated and acquired by the different units within the NFF to enhance their machine-learning models.

5.3.3. Existing materials

The areas of focus were crime in financial institutions and detective analytics, which are the core aspects of the study. The timeframe was vita, thus, papers published within ten years were considered, to gain insights into critical aspects such as the historical background and meanings associated with the phenomenon over time (Iyamu et al., 2016). Based on the recent use of detective analytics, only a small sample of the most appropriate and relevant literature could be gathered. This is not new as it has been experienced and argued in many IS studies (Glass et al., 2004; Brereton et al., 2007; Nyikana & Iyamu, 2023).

Existing materials often provide historical data that can be crucial for understanding trends and changes over time (Morgan, 2022). Also, existing materials provide background information and context that enhances the understanding of financial crimes within financial institutions. This includes a historical data overview that is crucial to understanding the trends and changes over time. The use of existing materials allowed for the performance of longitudinal and development analyses across different periods. Moreover, existing materials allowed us to benchmark collected data through semi-structured interviews, which helps in validating and comparing different views. The use of existing materials provided valuable context and offered access to diverse and comprehensive data sets.

5.3.4. Sources of materials

Materials published in journal outlets, books, conference proceedings, and the internet between 2014 and 2024 were gathered. 40 papers were collected from database sources such as AIS, EBSCOhost, Gartner, IEEE, and Emerald. 26 of the 40 papers were focused on detective analytics and 14 of the 40 papers focused on financial crimes. The sources were important because they instilled credibility and reliability in the data (Nyikana & Iyamu, 2023). Based on the focus and objective of the study, only 40 papers were relevant and used for the study.

The existing materials were sourced from most accredited sources which followed a defined validation process, ensuring a certain level of quality and reliability. Sources such as AIS, EBSCOhost, Gartner, IEEE, and Emerald are often rigorously reviewed by experts in the field, ensuring high credibility and reliability. These academic journals present detailed methodologies, ensuring the validity and reliability of the research. These papers are peer-reviewed and have undergone critical evaluation, which ensures that they are of great quality and consist of accurate information. The choice of sources was dependent on multiple factors which included the nature of the research question, the type of data required on financial crimes, the need for historical or current aspects of the crimes, and the level of detail necessary.

5.4. Fieldwork

The fieldwork was conducted in two areas; an organisation and a survey of the literature using document analysis techniques. The rationales for using an organisation and the literature are discussed in Chapter 4.

5.4.1. Fieldwork: Nikiwe Federal Finance

The data were collected from one of South Africa’s major financial institutions (NFF). The researcher obtained ethical clearance from the university to collect data to understand the nature of financial crimes that happen in South African financial institutions and, thereafter; examine the current preventative and mitigative measures. Furthermore, approval to interview employees within the organisation with knowledge of financial crimes and detective analytics was obtained from the organisation's internal legal team. Semi-structured interviews were conducted to collect data from the participants. 12 participants participated in the study. 6 of the participants were from the business departments and 6 were from the information technology (IT) department. A set of criteria for selecting the participants are presented and discussed in Chapter 4. A point of saturation was reached at 12 participants. In qualitative studies, a point of saturation is defined as the point or extremity where the researcher obtains the same information from the participants (Moser & Korstjens, 2018). The participants were obtained as follows:

Table 6.1: Demographics of participants

Role	Department	Level	No.
Reporting Systems Inspector	Business	Senior	1
Financial management support manager	Business	Senior	1
Associate Analyst	IT	Senior	1
Associate Investigator	Business	Senior	1
Legal Consultant	Business	Senior	1
Data Analyst	IT	Senior	1
Associate Analyst	IT	Senior	1
Associate Insurance Analyst	IT	Senior	1
Associate Bank Analyst	IT	Senior	1
Associate Reporting Systems Inspector	Business	Senior	1
Data Analyst	IT	Senior	1
Forensic Audit Manager	Business	Senior	1
Total			12

The interviews were conducted using the Microsoft Teams platform which was chosen as a preferred interviewing tool because everyone in the organisation has access to the tool, the tool is familiar to the participants and was granted by the internal compliance and risk department within the organisation. The selected participants had access to the Microsoft Teams application which is installed on their organisation's laptops as instructed by the internal compliance and risk department to protect the organisation from any security breaches and data leakages. The maximum length of all interviews was 30 minutes. This was considered a fair amount of time per interview to collect data during working hours and not inconvenience any employees in their daily operations. All collected data was stored in the university's data repository which can only be accessed by the researcher and the supervisor for the study. The data storage and backup plan were submitted and approved as part of the university's data management plan.

The researcher was able to reach out to the case's internal compliance and legal department to seek approval to conduct interviews for data collection. To obtain approval to conduct interviews, the organisation requested that the university and the participant sign a nondisclosure agreement, which stipulates that the organisation’s name and participants would be kept anonymous, and no sensitive data would be published. This was done to ensure that the university and the participant adhere to their ethical standards.

5.4.2. Document analysis

The document analysis technique was applied to gather documents which are also referred to as existing materials. The document analysis technique is used by researchers to evaluate physical and electronic materials such as peer-reviewed articles, books, newspaper articles, and organisational documents (Morgan, 2022). The data was collected using a set of criteria that included the areas of focus, detective analytics, publication timeframe, and credible sources. The timeframe of existing materials collected was ten years, this was to gain insights into the historical background and improvements with the detective analytics and financial crimes phenomenon over time (Iyamu et al., 2016).

5.5. Summary

The purpose of the overview of the data collection chapter was to outline how fieldwork was carried out and the overview of the selected case and documentation obtained. Semi-structured interviews were used to understand how access to the organisation was obtained and how the organisation is structured. Semi-structured interviews were conducted in the Nikiwe Federal Finance organisation. A total of 12 interviews were conducted, 6 from the business departments and 6 from the IT department. Subsequently, 40 papers were collected from scholarly databases. The next chapter presents the data analysis, which was conducted using the actor-network theory (ANT)’s four moments of translation.

CHAPTER SIX
DATA ANALYSIS

6.1. Introduction

The study's aim and objectives were presented in Chapter 1 and revisited in Chapter 4. The data collection using a semi-structured interview technique and document analysis was discussed in Chapter 4. This chapter presents the data analysis. The interpretivist approach was employed in the data analysis. The actor-network theory (ANT) was applied as a lens to guide the data analysis.

The remainder of this chapter is structured into three main sections. In the first section, an overview of the data analysis is provided. This is followed by the data analysis section underpinned by ANT's four moments of translation. The findings from the analysis are listed in the third section. Finally, the chapter is summarised.

6.2. Overview of the data analysis

As stated in Chapter 1, the research aims to develop a framework that can be used to guide the implementation of detective analytics to mitigate financial crimes. In achieving the aim, two objectives were formulated. The objectives depend on each other. The first objective is to understand the nature of financial crimes that happen in South African financial institutions. This leads to examining the current preventative and mitigative measures, if any. Thereafter, is the second objective, to investigate how the detective analytics tool can be deployed, to trace, track, and prevent financial crime in a financial institution, in South Africa.

In achieving these objectives, a South African financial institution is used as a case in the study. Data was collected from the organisation using the semi-structured interview technique. Based on the objectives stated above, the focus was on the use of detective analytics to mitigate financial crimes including the implications and use of the tool. Additionally, documents were gathered using the document analysis technique. The documents were used to complement the data gathered through the interview process.

The approach is introduced in Chapter 1 and discussed in Chapter 4. Nikiwe Federal Finance (NFF) is a pseudonym assigned to the financial institution that participated in the study. As discussed in Chapter 4, this was to avoid disclosing the organisation's identity and to maintain agreed ethics by the researcher and the organisation. A set of criteria was used to select participants. Also, each participant was assigned a codename to avoid the disclosure of identities: NKP01 – NKP12. Each document from the interviews was formatted, with page and line numbered. For ease of reading and referencing, a standard was formulated. For example, NKP01, 16:09 means an extract from participant number 1, page number 16, and line number

09 of the transcript from the participant. The documents gathered using document analysis were grouped into two categories namely, financial crime (FC) and detective analytics (DA). Each document was labelled: FCD01– FCD25 and DAD01 – DAD27 for the respective groups. For example, FCD01 10:20 means an extract from a financial crime-categorised document number 1, page number 10, and line number 20. The data obtained from both interviews and document analysis were combined for analysis purposes.

Following the interpretive approach, the thematic and hermeneutics techniques were applied to analyse interview data and documentation, respectively. The analysis was guided using the ANT as a lens. ANT was used to understand how networks are formed. Thereafter, the moments of translation as shown in Figure 6.1 were used, including the negotiations that occur in the organisation during financial transactions or activities. Callon (1984) explained that another critical aspect of ANT is that the theory focuses on shifting negotiation among actors, consciously or unconsciously.

6.3. Data analysis

As explained above, actor-network theory (ANT) was used as a lens to guide the data analysis. The analysis focused on how actor networks were created and the perspective of moments of translation. In the process, how negotiation shifted was also examined. Thus, the use of ANT is organised into two sub-sections, actor-network and moments of translation.

6.3.1. Actor-network

In ANT, actors are both human and non-human, and the network consists of actors (Callon, 1984). It is from this viewpoint Latour (2007) explains that actors and networks are not separatable. This is discussed in detail in Chapter 3. Therefore, an actor-network is a group of human and non-human actors based on shared common interests (Hsbollah et al., 2016). In this study, the groups are referred to as units, departments, or divisions. The alliance is formed consciously or unconsciously (Gao, 2005).

The first objective of the study is to understand the nature of financial crimes that happen in South African financial institutions. In doing so, three steps were followed. First, it was established that the actors associated with financial transactions such as the suspects, victims, and mitigators use various technologies, to either commit or mitigate financial crimes. In the second step, the networks (groups or units) involved were identified. The actors' roles were assessed in the third step.

The human actors are employees of both the business and IT departments of the organisation (Nikiwe Federal Financial). In the business department, the actors include business analysts, fraud investigators, business managers, and internal auditors. Software programmers, data analysts, solution architects, and IT managers are the human actors in the IT department. The non-human actors include software (tools used to commit or mitigate financial crime), data, big data, policies, and network protocols.

The actors are both internal and external to the organisation (or environment) where the crime was committed. The internal actors are employees of the Nikiwe Federal Finance (NFF), identified above. The external actors include suspects, customers, stakeholders, and public individuals. Internally or externally, the human and non-human actors performed different roles, in either committing or mitigating the financial crimes. These roles can be affiliated with the knowledge of how humans employ tools to navigate through processes to commit or mitigate financial crimes in organisations. Some of the participants stated as follows:

> "Currently, we are using the basic functions of data analytics tools, to mitigate financial crimes" (NK01,2:86). "Business managers are responsible for those customers who experience financial crimes and how the customers are transacting" (NK03,3:119-120).

There are networks of actors within the business and IT departments of the organisation (NFF). In the business department, there are units, which include compliance and enforcement, financial surveillance, risk management, prudential authority, and money laundering. In the IT department are the business solutions team, data analysts' team, artificial intelligence, and the machine-learning team. These departments and units form parts of the organisational structure. From ANT's perspective, the departments and units were consciously formed. Also, there were circumstances where employees from different departments and units constantly interacted on a common goal, which ANT refers to a network formed unconsciously. This was explained by some of the participants as follows:

> "Our purpose as the financial surveillance unit is to collect the cross-border financial crimes information from our reporting entities which may be banks and certain institutions that we have provided authority" (NK03,1:6-8). "As the prudential authority, our mandate is to supervise and regulate banks" (NK07,2:108-109).

The IT department, including its units, plays a critical role in mitigating financial crimes within the organisation. For example, software programmers create solutions using various tools to mitigate financial crimes. Additionally, the data analysts apply data analytics tools to understand patterns, anomalies, and reporting. While the solution architects provide enhancements and refinements to the tools used by both data analysts and software programmers, the IT managers ensure collaboration and corroboration among the units, towards mitigating financial crimes within the organisation. This includes detecting, monitoring, and tracking financial crimes. The activities of the IT department entail interactions.

Negotiations happen during interactions between actors (employees) to ensure fortified collaboration and corroboration. Owing to the different focuses and roles of the units, negotiation was not static but shifted. There are consequences in shifting negotiation, which include training and development, to ensure the employees involved in the process have the same understanding of the tasks.

Like the IT department, units within the business department have distinguished deliverables. At the time of this study, the team of business analysts was responsible for detecting anomalies in the data used during financial transactions, and the fraud investigators traced the perpetrators or suspects by following the actors. Additionally, the business managers enforce tools and processes to monitor and track financial crimes. The internal auditors and financial surveillance team also follow the actors through various controls and regulations to prevent or trace fraudulent activities within the organisation. According to some of the participants:

> "The risk and compliance team mitigates, and then internal auditors also ensure the controls are in place" (NK03,3:121-122). "We as business analysts have been providing financial transactions data for different departments such as the prudential authority and financial surveillance to detect crimes" (NK05,4:214-215).

Humans cannot act independently in either committing or mitigating financial crimes in the environment. Therefore, humans employ non-human actors to mediate and interact with the system, by internal and external activities. This makes the roles of non-humans critical in committing or mitigating financial crimes. For example, the auditors employ two tools called Promptool and Online Risk Manager to detect, monitor, and track financial crimes within the organisation. This includes the potential of a financial crime happening in any of the transactions conducted in the organisation. Two of the participants shared their views as follows:

> "We have a system that's called Online Risk Manager that we use to track the financial crimes" (NK06,3:163-164). "Promptool, the continuous monitoring tool is what we use in internal audit to detect failures in controls" (NK02,2:105-106).

The analysis presented above reaffirms that actors exist within networks, consciously by the organisation's design or structure or unconsciously based on individuals' interests. Also, a network does not exist without actors. Various steps and tools are involved in committing or mitigating financial crimes. For each of the steps or tools, activities happen, which are enacted through interactions. Due to the involvement of steps or tools including interactions, translation becomes paramount.

6.3.2. The moments of translation perspective

In ANT, translation goes through different moments. Thus, translation is described as the process where human and non-human actors transform and persuade each other (Baiocchi, Graizbord & Rodríguez-Muñiz, 2013). Callon (1984) categorises translation into four moments: problematisation, interessement, enrolment, and mobilisation, as shown in Figure 6.1. The process of translation in ANT is used in this study to describe how actors build alliances in forming networks (Bueger & Stockbruegger, 2017).

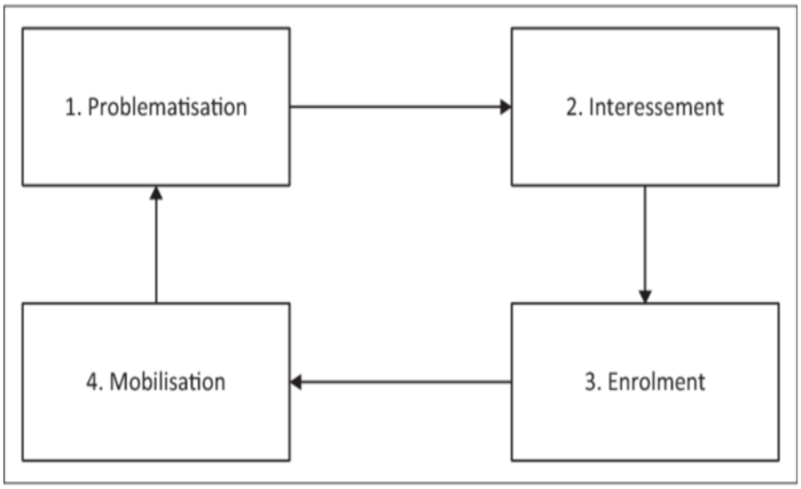

Figure 6.7: Four moments of translation (Callon, 1984)

The moments of translation, according to Sekgweleo and Iyamu (2022), assist in clarifying the actors' activities, actions, or interactions within various networks. In this study, the moments of translation are used for the data analysis to examine how activities and events concerning financial crimes were translated from one moment to another, by individuals and groups. This includes understanding the interactions that happened between the actors and how negotiation shifted during the process. In doing so, a summary was first provided, as shown in Table 6.1. Thereafter, the various moments were employed.

Table 7.1: Moments of translation

Problematisation	Interessement
In the organisation, mitigating financial crimes was problematised, primarily, at three levels. First, it is problematised at both business and IT departments' levels. Second, each department problematises the issue (potential or an incident) of financial crime to the unit heads. Third, the unit heads problematise it to their subordinates. Thus, awareness is created among the relevant personnel and groups. Based on this awareness, employees develop and show their interest. Also, different approaches or channels were used in problematising the issue of financial crimes in the organisation. Some groups used the statistical analysis system (SAS) to report and visualise financial crimes. The anomalies in transaction data were also used to problematise the issue.	Once the issue of financial crime was problematised, the actors involved gained a better understanding. Based on the understanding, including the insights that were provided, individuals and groups got interested. The interests of the employees were influenced by various factors, from personal to organisational necessities and obligations. However, not every individual or group shows interest. Consequently, some employees were compelled to show interest in complying with their contractual agreement with the organisation. ANT refers to this as an obligatory passage point (OPP) (Iyamu & Ibitomi, 2024).
Enrolment	**Mobilisation**
Individuals and groups (teams) are assigned roles and responsibilities in mitigating financial crimes in the organisation. The allocations of tasks are based on individual skills or teams' focus and deliverables. In ANT, the allocation and acceptance of tasks is referred to as enrolment (Johnson & Iyamu, 2019). For an actor to be enrolled into the network, negotiations happen. Actors employ various factors such as know-how and experience in their negotiations. From both the business and IT departments, actors were enrolled consciously based on their mandate and organisational structure that enforces the power and responsibilities to mitigate financial crimes.	Employees including the managers were aware that the more people involved in the drive to mitigate financial crimes, the more successful it becomes. Thus, managers in the business and IT departments undertake the task of inclusivity by mobilising other employees to comply with standards and policies, including the use of certain tools such as SAS. Mobilisation helps to strengthen the activity of the network (Latour, 2005). As a result, the spokespersons (managers) ensure that more people are inclusive. Also, individuals and groups undertake the translation of the tasks assigned to them, to gain a better understanding of the objectives and deliverables.

Moments of translation: Problematisation

Problematisation is the first stage in the four moments of translation. In the organisation, financial crime was a priority because of the detrimental consequences. As a result, mitigating financial crimes was problematised in the organisation. Additionally, actors relating to mitigating financial crimes such as people, processes, and tools were problematised. The problematisation of people was to ensure the involvement of the most authorities and qualified personnel. Processes were designed to streamline activities of mitigation; therefore, they were also problematised. Employees needed to be aware of and knowledgeable about the tools such as the SAS, and how to apply them to detect and mitigate financial crimes in the organisation.

Due to the severity of financial crime, it was problematised at various levels, vertically (from top to bottom) and horizontally (across the organisation). Vertically, problematisation happens at three main levels. The first level is strategic, where the senior management problematised the entities (financial crime, processes, and tools) to the heads of Business and IT departments. The second and third levels are operational. At the second level, the heads of departments problematise the entities to the teams and units. Thirdly, the heads of the teams and units share the information with individuals. It is at this level that the tools such as SAS are promulgated for use.

Significantly, problematisation at various levels helps to synergise and synchronise activities and processes towards mitigating financial crimes in the organisation. For example, through the discovery of types of financial crimes, a big data strategy was formulated to trace and track human movements that happened during and after financial transactions. The strategy helps to bolster confidence in investors and clients, which enhances competitiveness. Extract from the complementary data affirms as follows:

> “Big Data (BD) can help organisations identify opportunities, gain insights, enhance decision-making and transparency and promote innovation, productivity and competitiveness" (FCD03,2).

The organisation is investing in resources (human and non-human actors) to ensure that all transaction data is secure. This was revealed during the problematisation of a detective mechanism for mitigating financial crimes confronting the organisation. The problematisation of the mechanism provides ease and trust to their investors, clients, and potential clients to offer business to the organisation. Data security is not only for storage purposes but also to ensure safety while the data is in transit through technologies and devices. The organisation has implemented security mechanisms such as firewalls, authentication, data encryption and access control to detect and prevent infiltration by unauthorised actors. One of the participants employed in the IT department briefly explained as follows:

> “Other security measures are to strengthen the firewall and to strengthen security in terms of how we authenticate the customer using multifactor authentication” (NK03,2:57-59).

Infiltration and manipulation to commit financial crime remain consistent incidents confronting the organisation. Thus, to ensure sustainability, the organisation had to create mitigants using technologies to detect and prevent financial crime, iteratively. Consequently, problematisation is a continuous event in the organisation. Also, advances in technologies were constantly explored and implemented to detect and prevent new challenges posed by intruders. However, there are risks associated with some technologies such as online banking, mobile banking and the use of smartphones. In one documentation, it is stated as follows:

> “The adoption of new technologies exposes financial institutions to the risk of cyber fraud such as identity card theft, phishing, skimming, cyberstalking, cloning, vishing, malware and other forms” (FCD05,202).

Due to the challenges of some technologies used to mitigate (detect and prevent) financial crime in the organisation, collaboration and corroboration are critical. In addressing technology challenges, the organisation promulgated approaches that ensure regular updating of processes and training of individuals. The approaches consist of policies and standards to govern human activities purposely to improve efficiency and the selection of technologies. One of the policies is the financial crime risk management practice, which was introduced to the employees.

In enforcing collaboration and ensuring corroboration among employees in the units and departments of the organisation, emphasis is put on regular communication. Also, emails are frequently distributed to employees to assess their understanding and suggestions about new ways of detecting and preventing financial crimes confronting the organisation. Additionally, workshops and town halls are conducted among the employees involved in detecting and preventing financial crimes in the organisation. The workshops are primarily intended to raise awareness and teach employees how to apply detective technologies and policies. General meetings of the involved actors are referred to as town halls. At the time of this study, town halls were conducted once every month end by the internal audit and financial surveillance department, to update collaboration and corroborative efforts, and to brainstorm new ways of mitigating financial crimes. One of the participants stated:

> “That is why I said the other day in the town hall that people must apply professional scepticism when you look at any processes that can trigger financial crimes, such as the procurement process” (NK02,1:42-44)

Even though collaborative and corroborative efforts remained high on the agenda in mitigating financial crimes, problematisation is conducted at different levels. Primarily, this is because of the diversity involved in mitigating fraudulent activities, which includes the enforcement of processes, the application of technologies, and the roles of people. Also, the organisational structure defines the deliverables of business and IT departments, distinctively. For example, the business department ensures that all policies, procedures and mandatory requirements are met to ensure the investigations, monitoring and mitigation of financial crimes, according to the agreed action plans. One participant gave the following example:

> “According to the Financial Sector Conduct Authority (FSCA) and the National Consumer Commission, the business operational mandate is to warn the public and customers on financial crimes” (NK07,2:101-102).

The distinctive roles defined by the organisational structure instil ownership and responsibility among the employees. This has two primary implications: (1) It ensures that relevant stakeholders are aware of the problem and the security controls in place to detect and prevent financial crimes, and (2) It creates transparency in the activities of the entities providing controls and measures to detect and prevent financial crimes. These implications boost the confidence of the stakeholders, including shareholders and clients. Additionally, detection and prevention efforts draw various interests from different quarters such as employees, shareholders, clients, and governments.

Moments of translation: Interessement

Mitigating financial crimes was problematised in the organisation using various means and following different processes. Thereafter, the translation process continued, to get actors interested. Interessement is the second stage of the four moments of translation. Callon (1984) describes Interessement as the stage of the moments of translation where alliances of actors are sought. In essence, Interessement is concerned with gaining the actors' interest, including negotiating the terms of their involvement (Indergård, 2022). In NFF, mitigating financial crimes was problematised and interest was sought from employees in different departments and units. Various means, including the organisation's pursuit (such as growth and sustainability), were used in seeking the employees' interest. Despite the clearly stated pursuit of the organisation, the interest of the human actors was influenced by various factors. The influence could be categorised into three levels, primarily: organisational objectives, departmental or unit focus, and individual benefits or strengths.

The organisational objectives were used to entice the employees to be interested in its mitigation activities, which were to detect and prevent financial crimes. The 'selling point' to the employees was that financial crimes derail the performance, growth, and sustainability of the organisation, which adversely affects jobs. Additionally, loss of income through crimes affects financial incentives such as annual bonuses and salary increases. Choi et al. (2021) emphasised that organisational performance is relative to financial incentives and bonuses. These were worrying effects, which encouraged some employees to show interest in detecting and preventing financial crimes in NFF.

The ultimate interest emanating from NFF's objectives is to trace, track and prevent financial crimes before and as they occur; to trace is to discover by investigation, to track is to follow the trail or movement and to prevent is to stop the financial crimes from occurring. The organisation achieves these objectives by utilising advanced technologies such as data analytics tools to monitor its transaction data systems. Some employees' interests grew by anticipating how monitoring can help the organisation identify any anomalies and suspicious activities within the transaction data to mitigate the risk of a financial crime occurring. Additionally, some interests spanned foreseen action plans such as identifying the risks, creating solutions, implementing solutions, testing, and monitoring financial crime activities. This topic remains in discourse, as exemplarily documented:

> “Preventive strategies include policies, products and processes that are put in place to prevent a successful attack. The key goal of this category is to raise the bar for attackers by reducing their surface area for attack and blocking them and their attack methods before they impact the enterprise” (DAD13,3).

The organisation has assigned the action plans to different departments and units. Based on the objectives, the departments and units have obligations to foster the interest of the organisation. Although the business and IT departments had distinctive deliverables, their interests were corroborative. Thus, the business and IT departments and their subordinate units focused on safeguarding the organisation’s pursuit by managing financial transaction data and creating solutions for detecting and preventing financial crimes from occurring.

The IT department plays a crucial role in fighting financial crimes by leveraging technology and data management to prevent, detect, and respond to fraudulent activities. The key responsibilities include data protection, system security, monitoring, detection, compliance and incident response. This includes firewalls, encryption, intrusion detection systems, and secure access controls to protect sensitive financial data from unauthorised access and breaches. By combining these responsibilities, the IT department plays a crucial role in the prevention and mitigation of financial crimes, helping the NFF safeguard their assets and maintain trust with customers and stakeholders. Furthermore, the IT department provides training and resources to employees about security best practices, phishing prevention, and recognising fraudulent activities. Informed employees and customers are less likely to fall victim to scams or accidentally facilitate financial crimes. One of the participants from the IT department stated:

> “We offer training on fraud on how to identify red flags. Red flags are not always in the bigger things; it's not always the people who drive nice cars that you must do a lifestyle audit on, no! There are other things, such as change of character, small things that we overlook; so, not everyone knows the flags to look out for.” (NK02,4:172-176).

The tasks and responsibilities stated above were informed and determined by the requirements of the business. Both the IT and business departments are therefore compelled to engage in achieving and managing the business requirements. The engagement had two impacts. Firstly, it raises the levels of interactions and relationships between individuals and groups (units) in both IT and business departments. Secondly, executing the tasks enforces collaboration and corroboration between the IT and business departments and units, in NFF. At the time of this study, circumstances concerning the requirements leverage synergy towards a common goal of the organisation.

From the business department perspective, the interest was to assist the organisation in creating a robust framework for preventing and mitigating financial crimes. The framework contains key responsibilities, including policy development, risk management, training and awareness, compliance, internal auditing, monitoring, and reporting. The actors formed networks based on their understanding, which elicited their interests. The networks were consciously or unconsciously formed depending on whether it was influenced by personal objectives or organisational obligations. Irrespective of what triggered the interest, the involvement of actors (employees) was to commit or mitigate the financial crimes. A similar circumstance is documented as follows:

> "Extracting the hidden network structures among criminals and inferring their respective roles from criminal data can help law enforcement and intelligence agencies develop effective strategies to prevent crimes from taking place" (DAD19,2).

Primarily, individuals' interest in detecting financial crimes is influenced by either of two factors, benefits or strengths. Also, individuals influence one another in showing interest in the activities of building a detective approach to mitigate financial crime in the organisation. For example, based on the benefits of knowing the systems and controls in place, the employees were motivated to find loopholes for financial gain. In NFF, some employees were interested and only participated in the development of tools, policies and strategies to detect financial crimes that could be used to defraud the organisation. One of the reasons this occurs was explained by one of the participants as follows:

> "People feel entitled to whatever it is that they're stealing especially people who stayed in organisations for too long they feel like they deserve it and then now they are stealing" (NK01,1:18-19).

Some employees were using their knowledge of the organisation's processes and controls to create robust rules in SAS. This was to ensure that the reporting of financial crimes was improved. Furthermore, the organisation is creating a new solution called One Financial

Surveillance (One Finserv). It uses data analytics such as predictive, prescriptive, diagnostic, descriptive and detective analytics. This was confirmed by one of the fraud specialists:

> “Enhanced data analytics such as detective analytics is one of those things that we are working on as we are migrating to the one FinServ project because right now, we are looking at high-value transactions only based on the assumption that the higher the value the higher the risk” (NK05,2:69-72).

The Interessement can be affiliated with internal and external actors. Internally, the employees would be performing their day-to-day operations and tasks. Externally it is affiliated with customers, suspects, investors and other stakeholders. This can negatively or positively impact the interest in mitigating financial crimes. The negative effect could be because of negligence, because of human error, or intention to commit the crime. The positive impact is the organisation having the necessary tools, policies and controls in the environment to mitigate financial crimes. In one documentation, it was explained:

> “Anti-fraud activities have become a core business issue as the scale and the impact of fraud has grown in our digitally enabled world. Fortunately, innovative technologies such as monitoring, data analysis and predicting human behaviour can be used as preventive and detective measures” (FCD07,602).

Interessement is concerned with aligning the goals and interests of actors within the network. The alignment is therefore crucial for ensuring focus and stability, which motivates participating actors towards contributing to the network’s objectives (Indergård, 2022). Interessement is a fundamental aspect of ANT that explains how networks are built and sustained through the careful alignment of diverse actors' interests. It highlights the strategic efforts required to recruit and retain participants, ultimately contributing to the stability and success of the network. This helps to gain a deeper understanding of how humans can contribute to stability in enforcing detective and preventative measures, to mitigate financial crimes in the NFF organisation.

Moments of translation: Enrolment

Enrolment is the third stage of the four moments of translation. In ANT, enrolment is actors’ participation in a network’s events or activities, which occurs based on aligned interests (Callon, 1984). Through participation, alignment helps ensure that the network functions effectively and continues to work towards its objectives, including stability and growth. The process of enrolment in translation is crucial in forming and maintaining networks.

In the organisation (NFF), detective and preventive measures to mitigate financial crimes were conducted by teams of IT and business departments and units in collaboration. The collaboration entails layers of stages comprising various roles and actions. Consequently, the collaboration demands checks and balances among the teams and units because of the criticality of mitigating financial crimes in the organisation. Holcombe (2018) argued that checks and balances are essential in undertaking a critical examination of a process. According to Alisherovich and Ugli (2023:35), “internal control in banks refers to the system of checks and balances that are put in place to ensure that the bank's operations are in line with regulations, policies, and procedures”. Thus, checks and balances are enforced using more stringent roles and processes. Also, the checks and balances enable following the actors (humans or non-humans) in a financial transaction, to detect how and why it happened. This was discussed at an abstract level during the study due to the confidentiality associated with the details.

Individuals and groups (teams) are assigned roles and responsibilities in mitigating financial crimes in the NFF organisation. Amer and Al-Omar (2023) emphasised that effective mitigation of financial crimes requires seamless coordination and communication among the individuals and groups involved. Each role contributes to a multi-layered defence against financial crimes, creating a robust system of checks and balances. In the organisation, the seamlessness of the individuals’ and groups’ contributions was enacted using technology such as SAS and Oracle Business Intelligence Enterprise Edition (OBIEE). From both the business and IT departments, actors were enrolled consciously based on their mandate and organisational structure that enforces the power and responsibilities to mitigate financial crimes.

In NFF, power is critical in ensuring that the organisation can effectively detect and respond to financial crime. Power holds significant importance for three primary reasons. Firstly, some leaders in the organisation believe that authority over and control of resources give them the command of allocative capability and access to funding for advanced technology and hiring of skilled personnel. Giddens (1984) refers to allocative resources as a form of capability to generate command over objects, goods or material phenomena, and authoritative resources are types of transformative capacity for command over actors. Secondly, decision-making can influence the organisation’s policies and procedures. Thirdly, strategic vision enables the development and execution of long-term goals and initiatives to enhance how the organisation detects and prevents financial crime (Haslam et al.,2020; Sartania, 2021). This topic remains in discourse, as exemplarily documented:

> “Financial institutions continue to work relentlessly to advance their capabilities, forming partnerships across institutions (including governmental bodies) to share insights, patterns and capabilities” (FCD12,1).

Monthly meetings, updates, and collaborative efforts help ensure that the organisation’s financial crime prevention strategy is comprehensive and effective. The financial crime prevention strategy for NFF is based on safeguarding transaction data, maintaining regulatory compliance and protecting the integrity of the organisation. This includes conducting risk assessments, developing policy and procedures, training and awareness, internal audit, monitoring and continuous improvement. This determines the participation of the employees and the allocation of tasks, towards achieving the strategy. The strategy is focused on minimising risks and enhancing the resilience of mitigating and preventing financial crimes. One of the participants stated:

> “There is a vulnerability assessment that we do before we do fraud risk assessments. It's like our first phase in terms of our methodology and financial crime prevention strategy” (NK02,2-3:109-111)

The IT department plays a crucial role in detecting and preventing financial crimes within NFF. The enrolment of the actors from the IT department is, primarily, based on the deliverables of each of the units, which include implementing and managing security measures, monitoring threats, tracking incidents, and ensuring the integrity and confidentiality of the data involved in financial transactions. In doing so, collaboration with individuals and units is essential and data analytics are employed in fulfilling collaborative tasks. One of the participants explained the significance of using data analytics tools to track and trace financial crimes during investigation by the business teams:

> “We also have a daily report that we are doing to ensure that if there's any suspicious transaction that anomaly is inquired and sent to the investigations team” (NK05,1:29-31).

In conjunction with the IT department, the business department plays a significant role in detecting and mitigating financial crimes within the organisation. The department’s responsibilities include implementing practices that prevent financial crime and ensuring that the organisation operates within legal and ethical boundaries by developing and enforcing internal controls and procedures to prevent and detect financial crimes. This includes the segregation of duties (SOD), risk management, fraud prevention strategies, collaboration and coordination. The importance of SOD is to strengthen internal controls by ensuring that every role and authorisation about transaction data is monitored and tracked by a person of higher authority according to the organisational structure. This creates oversight by multiple people which then ensures that the organisation has different perspectives to prevent and identify fraudulent activities. According to Alisherovich and Ugli (2023), by dividing responsibilities among different individuals or departments, SOD helps reduce the risk of errors, conflict of interest, and fraudulent activities. One of the participants stated:

> “We did a financial transactions anomaly report and sent it because we only perform data analysis, and we do not conduct investigations” (NK05,2:16-17).

A robust environment is created by the business units to contribute to the organisations’ overall integrity and operational effectiveness. A robust environment in NFF is defined as a resilient application or system that governs and mitigates risks, ensuring the accuracy, completeness, and reliability of transaction data for reporting and preventing financial crimes. For example, the use of SAS creates a robust environment for the data analytics team in ensuring that they conduct their reporting using accurate, complete, and reliable transaction data which feeds from all financial transactions of the organisation. SAS tracks all transaction data using categories to classify the type of transaction and the intended purpose for ease of tracing and tracking. One of the data analytics specialists stated as follows:

> “We use SAS enterprise to do further analysis of the transactions if, for example, a particular category looks inflated in the report. Then they would dig deeper using our SAS tool and then we would know if there's a series of transactions inflating that particular category” (NK09,2:96-99).

Every employee has at least, a role and responsibility in ensuring that the mandate and financial crime prevention strategy are successful. From the business department perspective, units are assigned different roles based on their specialities and organisational requirements. This covers policy development and updates and ensures risk management, including conducting risk and vulnerability assessments. Moreover, the business units are responsible for providing training and awareness. Other areas through which employees in the business department participate in detecting and mitigating financial crime include conducting internal audits, and preventing, monitoring, and reporting anomalies that could lead to financial crimes. In alignment with the business department, the IT department also has different tasks that provide support to the business to ensure that the data used for financial transactions is available, safe and reliable. This is done by assigning different roles such as developers, data analysts, system administrators, database administrators, and cyber security specialists.

Moments of translation: Mobilisation

Mobilisation is the fourth stage of the four moments of translation (Callon, 1984). Iyamu and Ibitomi (2024) refer to it as the point or stage where all actors are enrolled successfully into the network. For actors to be involved and fully participate in preventing and mitigating financial crimes in their various units (networks), mobilisation needs to happen. Latour (2005) emphasises that mobilisation has the strength to create and aid the execution of activities in a powerful way, within networks. In NFF, business and IT departmental managers are responsible for mobilising employees to embrace the goals of mitigating financial crimes. This is a mandate bestowed on the managers as prescribed by the organisational structure. This was also confirmed by one of the participants as follows:

> "When we do our fraud risk assessments and awareness campaigns there is this tool that we use; the tone starts at the top management to discuss how we implement anti-fraud policies, training and how to perform data analysis because it is very important" (NK04,3:155-157).

As of the time of this study, the organisation had a mandate to mitigate financial crimes. Thus, detecting and preventing financial crimes was an ongoing activity rather than a project. Those responsible for detecting were not necessarily focusing on prevention. However, there was an overlap in their duties. Hence, corroboration and collaboration between the responsible authorities were critical. Negotiation between the teams continued to shift to ensure smooth collaboration and effective corroboration. The corroboration and collaboration were enacted by following the actors. As a result, there was a continuous mobilisation of employees in the organisation. The activities of mobilisation were conducted by establishing a robust framework which contains key responsibilities, including policy development, risk management, training and awareness, compliance, internal auditing, monitoring, and reporting. Furthermore, various strategies were integrated to detect, prevent, and respond to financial crimes in the organisation.

The mitigation of financial crimes involves a multi-faceted approach which includes the business and IT departments. In NFF, various approaches are used in mobilising employees, including stakeholders, in mitigating financial crimes. This includes strategic and operational approaches, which focus on regulatory practices. This is aimed at continuous improvements. Additionally, the goal of mobilising using the various approaches is to ensure that a robust strategy in the form of a digitalised system is in place to prevent and mitigate financial crimes. One of the financial surveillance specialists stated:

> “The financial entities who are accountable institutions need to have a risk management plan so that they can identify financial crimes and know their clients” (NK10,1:33-35).

Different stakeholders work collaboratively in building a comprehensive framework for preventing and mitigating financial crimes in NFF. This includes managers and employees in business and IT departments, clients who report suspicious activities or transactions, and law enforcement agencies. Based on the involvement of diverse actors, mobilisation is coordinated. Both the business and IT departments have delegated spokespersons. The tasks of the spokespersons are guided by requirements, which were formulated based on the organisation’s objectives and the government legislature. The legislative bodies and regulatory agencies pass laws and regulations, while the financial institutions adhere to these laws by implementing internal controls to track, trace and monitor financial crimes. One of the participants explained as follows:

> “In terms of what's currently being reported, we work closely with the Financial Intelligence Centre (FIC), with the banks, and the National Consumer Commission (NCC), because the NCC has demanded to know what we deal with specifically in terms of the Consumer Protection Act” (NK07,1:38-41).

In addition, there are private and industry groups such as the South African Risk Information Centre (SABRIC) that constantly and consistently monitor industry-wide financial crimes and deliver reports for public awareness and transaction monitoring tips. In NFF, the mobilisation of employees in preventing and mitigating financial crimes is informed by evidence obtained through digitalised systems such as the use of financial surveillance. One of the financial surveillance specialists affirmed:

> “There is a department in FinServ called the compliance and enforcement. That division is responsible for doing the investigation and also the necessary sanctions related to the financial crimes and other cross-border matters” (NK03,1:14-16).

Heads of units tasked with detecting and preventing financial crimes in the organisation mobilise other employees, including stakeholders and clients, to participate in preventing financial crime. ANT refers to these drivers as spokespersons (Callon, 1984). Iyamu (2024) suggests that the spokesperson can be nominated by the organisation or self-appointed. As spokespersons, the heads of the units use various means such as communication and training in mobilising other actors. The approach enables inclusiveness and fortifies efforts to corroborate and collaborate in detecting and preventing financial crimes in the organisation.

Effective communication is crucial in the efforts to mobilise other actors. The effectiveness is based on shifting negotiation that is imbibed in the communication between the spokespersons and other actors. Shifting negotiation allowed the actors to contribute their views and offer solutions. Therefore, the involved personnel (actors) understand each other better in terms of the action they have to perform at various times and stages. Another factor that makes communication effective is that it is structured and, from reliable sources, is ascribed to the organisational structure.

Also, the stakeholders are updated through regular meetings and briefing sessions. In the meetings and sessions, clients are encouraged and allowed to raise concerns or report suspicious activities. This is a state of shifting negotiations and practical consciousness. Giddens (1984) describes practical consciousness as a state which consists of the things actors know tacitly but are unable to give direct discursive expression. According to Iyamu (2024), employees' actions often conducted in organisations intertwine in their minds as knowledge gained through practical consciousness.

The employees are trained and afforded the relevant resources to use, in either detecting or preventing financial crime within the organisation. This encourages the employees to be more inclusive in the strategic or operational aspects of financial crime. The business and IT heads of departments are aware that the more people are involved in the drive to mitigate financial crimes, the more successful it becomes. Thus, managers in the business and IT departments are assigned the task of inclusivity by mobilising other employees to comply with standards and policies including the use of certain tools such as SAS and OBIEE. This topic remains in discourse, as exemplarily documented:

> “The board of directors of an organisation fulfils its role effectively and is involved with integrity, promoting an appropriate Tone at the Top (TATT) and an ethical programme from the highest level. This could be complemented by promoting organisational accountability to the general public, that is, safeguarding the public faith of key users, including shareholders or owners” (FCD13,12).

In mobilising employees, including stakeholders and clients to participate in reporting and preventing financial crimes within NFF, the organisation has to consider how different actors and their interactions shape the effectiveness of these efforts. Standards, procedures, and protocols were created and enforced for all actors to abide by in ensuring consistency across the networks in their heterogeneity. In making mobilisation easier, for both the business and IT departments, technology systems such as SAS and OBIEE were integrated with existing processes for reporting and monitoring. The monitoring allowed actors to be followed and made networks (groups and units) responsible for preventing financial crimes more effective. This includes regular audits and individual performances in their respective roles. One of the participants declared:

> “We report to information flow if it's a report on incorrect reporting, or we report to financial operations if it's something that is an investment-related crime. We don't have the authority to deal with the authorised dealers or the client directly. So, whatever we pick up we report to the relevant division, and they run with it” (NK12,1:31-35).

To ensure more inclusivity, individuals and groups undertake the translation of the tasks assigned to them, to better understand the organisation’s objectives and deliverables. Monthly meetings and awareness sessions are conducted to keep all employees informed about changes in policies, emerging threats, and industry best practices. This could have been digitalised to improve mobilisation. Also, the monthly engagement sessions allow employees to collaborate and share information, which improves the ability to mitigate financial crimes in NFF. Moreover, this allows employees to develop and enhance strategies based on the evaluation of the current state. One of the data specialists observed a gap in the system:

> “The way our data is so complex, we are talking about big data; it’s not easy for one person to pick up an anomaly unless it’s really a big transaction value and maybe we will have such a model as time goes, but you will never know that it’s wrong reporting from our side” (NK05,3:161-164).

Employees, stakeholders, and clients are mobilised using a framework. The framework is comprehensive because it integrates many facets of the NFF, including strategies, tools, and policies aimed at detecting and preventing financial crimes. This effort is characterised by the deployment of advanced technologies such as SAS and OBIEE, rigorous policy frameworks, and enhanced training programmes used in teaching the mitigation of financial crimes. However, continuous improvement is essential to address challenges and adapt to emerging threats by focusing on technological advancements such as the new Surveillance One Finserv project which has enhanced data analytics such as detective analytics to discover an anomaly as and when it happens.

6.4. Findings and summary

As introduced in Chapter 1 and discussed in Chapter 3, the actor-network theory (ANT) was applied as a lens to guide the data analysis. It was considered most suitable to achieve the objectives of understanding the nature of financial crimes that happen in South African financial institutions. This led to examining the current preventative and mitigative measures, if any. Thereafter, the study investigated how the detective analytics tool can be deployed to trace, track, and prevent financial crime in a South African financial institution. Using empirical evidence from the participants, the analysis focused on the nature of financial crimes from individual experiences and opinions.

From the analysis presented above, seven factors were found to influence the use of detective analytics to mitigate financial crimes in organisations. The factors are as follows; (1) Collaboration; (2) Corroboration; (3) Internalisation; (4) Externalisation; (5) Digitalisation; (6) Organisational structure; and (7) Integrated analytics. Also revealed from the analysis is the fundamental relationship between the factors, indicating that the factors do not operate in silos but are dependent on each other.

CHAPTER SEVEN
INTERPRETATION OF FINDINGS

7.1. Introduction

The findings from the data analysis using actor-network theory (ANT) are presented in the previous Chapter (6). The findings were interpreted using activity theory (AT), as presented in this Chapter. The interpretation is crucial in making sense of the findings, as different perspectives can enrich understanding and highlight various implications. The interpretation leads to the discovery of insights and a deeper understanding of the findings. Loke et al. (2021) stated that information is interpreted to determine what was discovered during data analysis. Based on the interpretation, a framework was developed, which can be used as instrumentation for employing detective analytics, for mitigating financial crimes.

This chapter is divided into two main sections. The first section contains an overview of the interpretation. This is followed by the interpretation of the findings. Finally, the chapter is concluded in the last section.

7.2. Overview of the interpretation

From the analysis presented in Chapter 6, seven factors were found to influence the use of detective analytics to mitigate financial crimes in organisations. The findings were interpreted using activity theory (AT). In using AT, the subjective approach was applied. This was to (1) gain insights into the relationship between the factors that influence the mitigation of financial crimes in an institution and (2) develop a framework that guides an understanding of how detective analytics can be deployed to trace, track, and prevent financial crime in a financial institution. Thus, the interpretation of the findings followed two steps. In the first step, the relationships between the factors (findings) were established. Meanings were associated with the factors in the second step. The AT and subjective approach were utilised in both steps of the interpretation. Although AT and the subjective approach are comprehensively discussed in Chapters 3 and 4, further explanations are provided in subsections 7.2.1 and 7.2.2, respectively.

7.2.1. Activity Theory

The Activity Theory (AT) is used in this study as a lens to guide the interpretation of findings with a focus on how detective analytics is used as a tool to assist in the mitigation of financial crimes in financial institutions. Engeström (2000) describes AT as a tool that is used to understand human actions and their interactions within a socio-cultural context. The theory emphasises that human activities cannot be isolated and are part of complex systems that encompass different components and relationships (Peim, 2009). The components of AT are tools, subjects, rules, community, division of labour, and object, as shown in Figure 7.1. The theory, including its components, is comprehensively discussed in Chapter 3. The discussion is revisited to reintroduce its use as a lens for interpreting the findings.

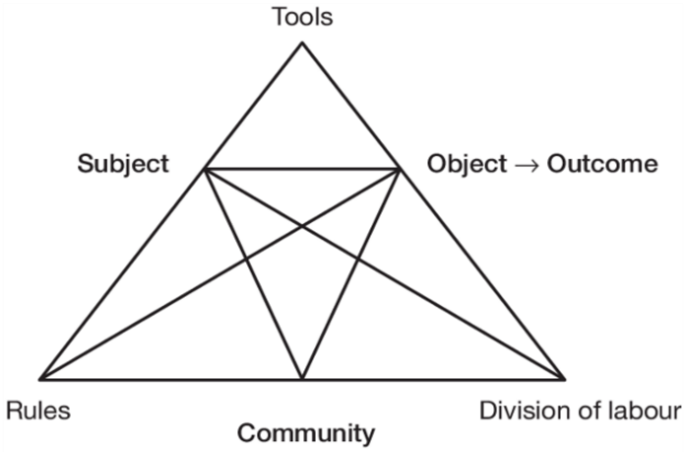

Figure 7.8 Activity Theory Model
(Nardi, 1996)

Tools are artefacts that mediate or are used to facilitate an activity system. According to Kaptelinin and Nardi (2009), the artefacts can be physical tools such as software and computers. This makes tools useful in understanding how artefacts are used to commit or mitigate financial crimes. The subject is the human actor who consciously performs an activity (Jonassen & Rohrer-Murphy, 1999). Rules are defined as the norms and regulations that govern how the activity is performed. These rules can be formal or informal and govern actors' relationships and interactions in performing an activity (Benson et al., 2008). A community is a social group or environment within which an activity is performed (Engeström, 2009). According to Iyamu and Shaanika (2019), the division of labour is a way in which tasks and responsibilities are assigned to community members. The outcome reflects the effectiveness of the activity in achieving its goals and can lead to changes in the object or in the activity system itself (Iyamu, 2020).

7.2.2. Subjective approach

The subjective approach allows reasoning through which meanings are associated with factors including entities, objects, and events. Oakley (1997) emphasises that the subjective approach is important in understanding individuals' perspectives and experiences of social phenomena. Thus, the subjective approach was used to gain insights into the different perspectives of how financial crimes occur, including how detective analytics can be applied to mitigate financial crimes in financial institutions. The subjective approach was employed from the interpretive perspective as shown in Figure 7.2.

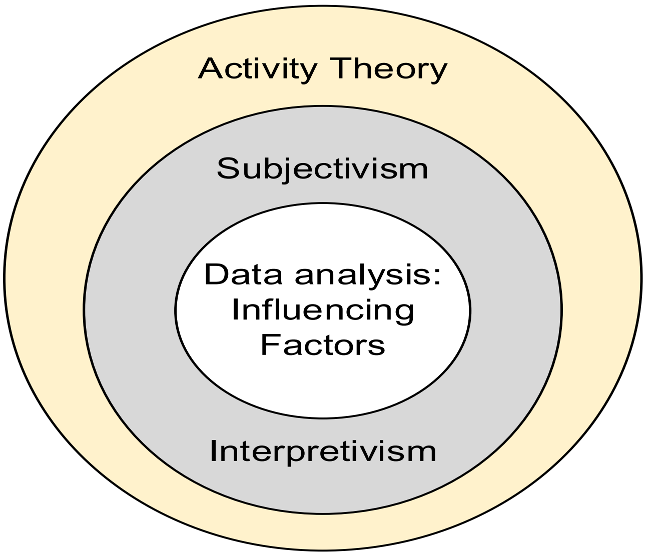

Figure 9.2: Interpretation of the findings

The interpretive approach is a paradigm that entails approaches such as subjectivism. The paradigm allows various realities of views and experiences of individuals within their social and cultural contexts (Koskosas, 2008). Interpretivism emphasises understanding the meanings and experiences of financial crime activities and the processes followed in mitigating them. When interpreting findings, the interpretivist viewpoint involves reflecting on the participants' viewpoints and recognising the processes and environmental structures, including the realities that exist in using detective analytics to mitigate financial crimes.

7.3. Interpretation of the findings

From the data analysis, seven factors were found to influence the use of detective analytics to mitigate financial crimes. The factors were presented in Chapter 6 and revisited here, for interpretation purposes. The factors are as follows; (1) Collaboration; (2) Corroboration; (3) Internalisation; (4) Externalisation; (5) Digitalisation; (6) Organisational structure; and (7) Integrated analytics. A two-step approach is employed for the interpretation of the findings. The steps are presented and discussed in subsections 7.3.1 and 7.3.2, respectively. The first step maps the factors (findings from analysis) with AT components. In the second step, the influencing factors are linked, the attributes are established, and through subjectivism, AT components are used to examine the factors and their attributes.

7.3.1. Step #1: Mapping the influencing factors

The first objective of the study is to understand how financial crimes happen in South African financial institutions and, thereafter, examine the current preventative and mitigative measures. In doing so, data was collected and analysed revealing seven influencing factors. To understand how financial crimes happen in the organisation, the factors were examined using AT. This was done because of two reasons. Firstly, the influencing factors have a relationship between them as they do not operate in silos. Secondly, AT components are mapped with the influencing factors. This is to establish how the factors manifest by examining their dependence on each other, as shown in Figure 7.3.

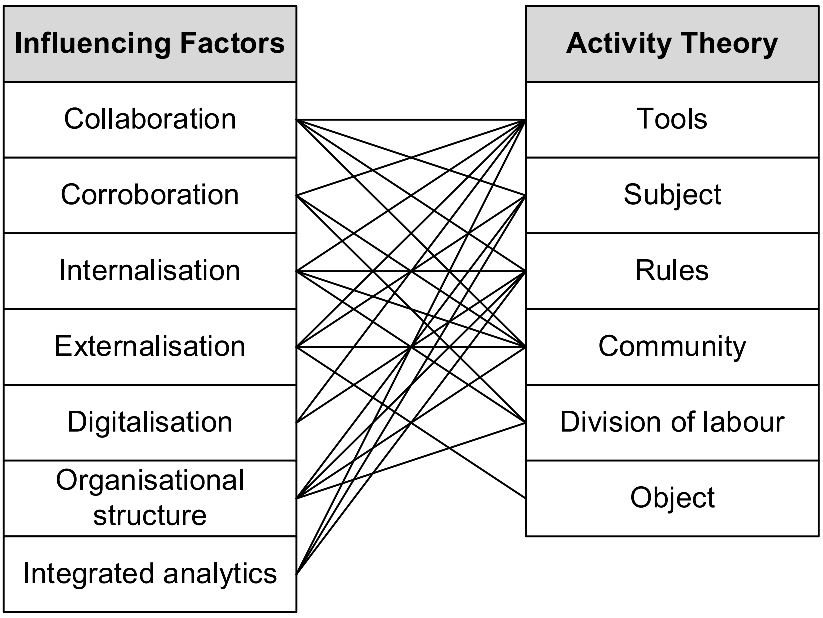

Figure 10.3: Mapping influencing Factors with AT

The mapping is as follows:

i. Collaboration: In collaboration, tools are used. Subjects (actors) are involved in the collaboration. Rules govern collaboration efforts. According to Sutrisno et al. (2021), collaboration is an alliance between two or more individuals to achieve a common goal. Thus, the community is a critical component of collaboration.

ii. Corroboration: Corroboration entails division of labour, which happens within a community setting using various tools. Kammerer, Gottschling and Bråten (2021) explained how corroboration helps to predict information from various sources.

iii. Internalisation: Internalisation requires the use of tools. Rules are applied in the use of tools, including how the division of labour is conducted within a community to internalise a process or an activity. Greulich, Lins and Sunyaev (2020) suggest that internalisation is the process of absorbing both tacit and explicit information by the rules of the environment.

iv. Externalisation: tools are applied by subjects (actors), to execute an action. It is purposely to achieve an outcome, legitimately or illegally. According to Sert and Alparslan (2022), externalisation helps to define how an organisation operates with external individuals including detecting how confidential internal activities and processes are exposed. Perpetrators create an external community to work together to commit financial crimes within the organisation.

v. Digitalisation: Digitalisation is enabled and supported using various tools. Also, rules are enforced to implement and digitalise processes and activities. Bargoni et al. (2024)

argued that, within rules, digitalisation allows an organisation to build strategic capabilities.

vi. Organisational structure: This is governed using a set of rules. Each structure consists of subjects. In carrying out tasks or actions, the subjects form a community, and a division of labour takes place. The organisational structure outlines the coordination of the organisation's operations including the responsibility bestowed by levels of authority (Nwankwo et al., 2022).

vii. Integrated analytics: The integration of analytics is conducted by subjects using various tools and adhering to rules. The use of integrated analytics provides an organisation with a holistic view (Schaefer & Makatsaria, 2021).

It was critical to map the factors because it reveals the relationship and their effects. Understanding the influencing factors relationships leads to gaining better insights into how the factors manifest. This helps to ease the tracing, tracking, and monitoring of financial crimes. Also, the relationships between the factors assist in automating processes and formulating rules to prevent and mitigate financial crimes in an organisation.

7.3.2. Step #2: Detective Analytics Framework

The data analysis revealed the fundamental factors that can influence mitigating financial crimes in an organisation. Based on the influencing factors, a framework is developed, as shown in Figure 7.4. The Framework depicts the links and dependence between the factors. Arrows are used to illustrate links and dependence between the factors. This indicates that the factors do not operate in silos and, therefore, interact with other entities. The factors are connected and depend on each other. Also, the influence of the factors is facilitated by various attributes. The attributes include communication, control, requirements, synergy, leverage, and intrusion. The attributes were revealed in the data analysis.

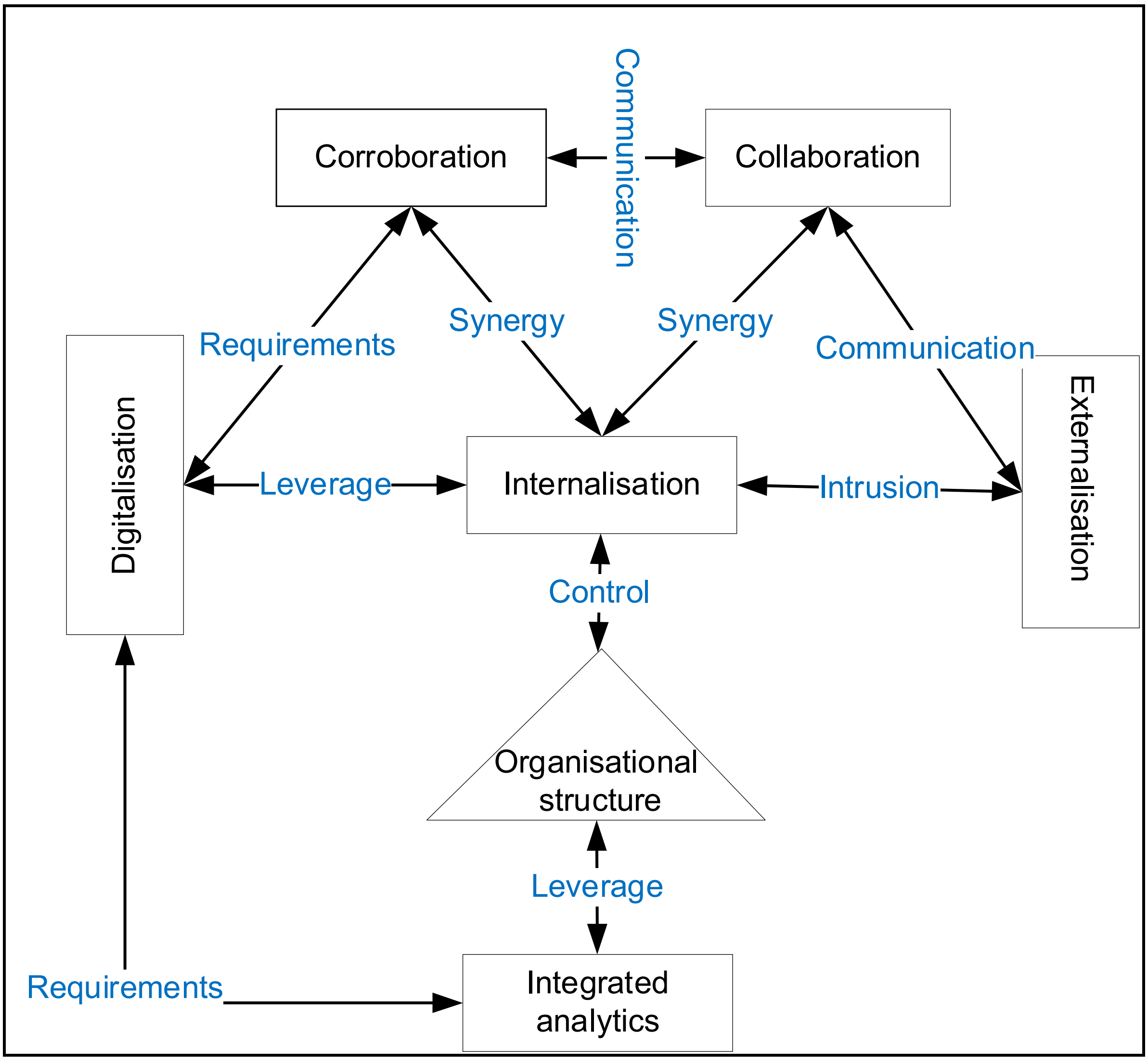

Figure 11.4: Detective analytics factors and attributes

7.3.2.1. Collaboration

Collaboration between departments, units, and individuals responsible or tasked with mitigating financial crimes in the organisation is critical. Thus, for collaboration to be successful, there needs to be synergy, tighter coordination, and streamlined communication between the actors. This is ensured through monthly meetings, updates, and information sharing as revealed from the data analysis. These are planned intentional actions that can enable the corroboration of information and strategic efforts among the units and actors to mitigate financial crime. The collaborative effort is therefore enforced using various tools, within rules, by members of the mitigating community in the organisation.

Tools: In enforcing and ensuring collaboration among employees in the departments and various units within the organisation, emphasis must be on the use of tools. Various tools must be used for two primary reasons. Firstly, to build layers of access during financial transactions. This is to make it difficult for intruders or perpetrators and colluders. Secondly, the tools must be constantly refreshed to counter intrusion and mitigate crimes. However, Nicholls et al.

(2021) suggested that tools can be used negatively or positively. As noted from the analysis, different tools, policies, and strategies were developed to detect financial crimes that could occur in the organisation. In NFF, the primary focus should be to communicate, collaborate, detect, monitor, and track financial crimes using automated rules. This will allow actors and their activities (transactions) to be traced and monitored internally and towards external sources.

Community: The success or maturity of a collaboration hugely depends on the uniqueness of the community. It is therefore crucial for the community to be in synergy. According to Fontana et al. (2022), a key element of collaboration is for the actors to belong to a community. As revealed from the data analysis, both the business and IT managers ensure collaboration among the units towards mitigating financial crimes within the organisation. This includes detecting, monitoring, and tracking financial crimes. In achieving these critical actions, collaboration between the different individuals in their respective units was essential and data analytics were employed in fulfilling collaborative tasks. Additionally, for the collaboration to be successful, there must be layers of synergic roles and actions.

Subject and rules: In mitigating financial crimes, collaborative efforts subjects (actors) and rules play critical roles. On the one hand, the collaboration must be governed by the actors using various rules. On the other hand, the actors must adhere to the governing rules. As the actors create rules that govern them, a more cohesive and effective collaboration is ensured, which forties better synergy and communication. Balcerek et al. (2021) state that rules are enforced in organisations to ensure that all procedures are followed accordingly to achieve the desired outcome of the collaboration. As revealed from the analysis, there were rigorous policy frameworks which NFF adhered to in creating the rules used to build any solutions for mitigating financial crimes. In NFF, the rules allowed the actors to enforce processes and controls of mitigating tools such as SAS.

7.3.2.2. Corroboration

Corroboration certifies information and material evidence between actors in their quest to mitigate financial crimes in an organisation. Also, corroboration strengthens actions by individuals and units. Lacity et al. (2021) explained how corroboration asserts and gives credence to actions and decision-making. Corroboration within a community consisting of IT and business personnel, where specific roles and responsibilities including the division of labour (task allocation) are assigned using tools such as detective analytics, increases the strength in mitigating financial crimes. Thus, a synergy between the IT and business departments must be ensured, and requirements to gather corroborative evidence outlined. It is from a similar perspective Kiili et al. (2020) suggested that corroboration effort avoids biases.

This helps to internalise and digitalise processes and activities geared towards mitigating financial crimes using detective analytics.

Community: To corroborate support and teamwork is a requirement from the community. As revealed from the data analysis, corroborative efforts remained high on the agenda of mitigating financial crimes. However, the NFF still struggled to detect, motor and track financial crimes. The community was tasked to corroborate and invent new solutions, policies and frameworks to mitigate financial crimes. The organisational structure defines the deliverables of business and IT departments, based on distinctive requirements. Therefore, a community should exist based on the different mandates that each department and unit is assigned. The internalisation processes and procedures guide how the community operates.

Division of labour: From the AT viewpoint, division of labour is the roles and responsibilities of people in a community (Siemonova, 2017). Division of labour plays a critical role in ensuring that all community members are allocated tasks and responsibilities in different activities to trace, track, and prevent financial crimes in the organisation. Allocation of tasks should be a process that ensures skills and the specialisation of individuals or teams align with focus and deliverables.

However, division of labour can be associated with the power dynamics and status of the actors within a community (Murphy & Rodriguez-Manzanares, 2008). As noted from the data analysis, both the business and IT departments had personnel guided by organisational requirements. Furthermore, the heads of units should be tasked to communicate with stakeholders and clients to participate in the process of preventing financial crime. In NFF, managers in the business and IT departments were assigned the task of inclusively tasking employees within their departments and units to comply with standards and policies, including the use of certain tools such as SAS and OBIEE.

Tools: From the AT perspective, tools mediate the activities of the actors towards an object (Iyamu, 2024). In the context of this study, mitigating financial crimes is both an outcome (technology solution) and an object. NFF employees use tools to carry out their day-to-day operations. Tools are used to achieve an outcome (Futerman, 2015). As noted from the data analysis, NFF uses tools such as data analytics to understand the patterns and anomalies in transaction data. Moreover, tools assist both the IT and business departments in corroboration based on their respective units' assigned tasks and action plans. The key responsibilities of using tools in NFF are to ensure data protection, system security, monitoring, detection, compliance and incident response. The tools provide a platform for corroboration and reinforcement of controls in place to ensure the detection, monitoring, and tracking of financial crimes.

Corroboration can yield positive or negative results. The positive effect is the verification and confirmation of all activities conducted within the organisation which provides evidence and an audit trail to confirm the activities. Negatively, an employee knowing the processes can easily infiltrate the evidence and audit trail.

7.3.2.3. Internalisation

Internalisation explicitly focuses on an organisation's processes and activities, such as policies and requirements (Abusharbeh, 2024). This includes operations and strategy activities. The Framework (Figure 7.4) depicts that internalisation is influenced by other factors such as (i) collaboration and corroboration with entities to ensure synergy; (ii) digitalisation, to leverage both IT and business processes and requirements; (iii) monitoring and preventing intrusion from external sources; and (iv) organisational structure control of internal processes and activities. According to Bos-Nehles et al. (2017), the control ensures and administers the jurisdictions, authority, and governance of the internal processes of an organisation. Internalisation is shaped by the tools used, governing rules, and how the division of labour is conducted.

Tools: In AT, a tool can be tangible or intangible, and it is used to mediate between a subject and an object in an activity (Hasan & Pfaff, 2012). In a further clarification, Iyamu (2024:232) explains that "tangible tools can refer to items such as machines and instruments, whilst intangible tools can refer to procedures, languages, or laws". Thus, a tool can be used by an organisation for internalising processes towards achieving its goals and objectives (Kaur et al., 2023). As revealed from the data analysis, using tools such as SAS and OBIEE ensures that NFF has control and standardised internal processes, which helps in monitoring and reporting anomalies in the transaction data.

The tools also aid the internal processes to leverage digitalisation to create ease of conducting all activities and processes using electronic technologies. However, it was noted by Muñoz et al. (2022) that for internalisation to be a success there needs to be synergy and synchronisation between the tools used in the organisation. Furthermore, the weakness in internal process controls may lead to perpetrators easily bypassing security and any firewalls blocking outside access into the organisation.

Rules: From an AT perspective, rules can be explicit or implicit, defining what is acceptable or not in an environment (Karanasios, 2018). Malik et al. (2022) emphasise the role that rules play in controlling and influencing employees to ensure that all operations are conducted as intended. Moreover, rules in NFF as noted from the data analysis, facilitate how digitalisation should be leveraged for all internal activities and processes. Pillai and Helberg (2021) argued that rules govern how applications and systems are configured to ensure that intrusion is swiftly detected internally.

However, it was noted from the analysis that most applications and systems operate in silos and therefore lack compatibility, which enables perpetrators to attack and commit financial crimes. This is critical in applying detective analytics for mitigating financial crimes. A group of employees (community) is regulated by policies and procedures that govern how members conduct their activities and processes. This, however, can also be infiltrated either positively or negatively: Positively by adhering to the internal policies and procedures and ensuring that all activities are conducted within the defined rules. The negative impact is an insider (employee) sharing these rules to an outsider to infiltrate the NFF, using tools.

Division of labour: Division of labour in AT is assigning tasks, roles, and responsibilities to individuals partaking in an activity (Nehemia-Maletzky et al*.,* 2018). Consequently, internalisation embeds the division of labour approach to cover areas of importance in mitigating financial crimes. This means that roles and responsibilities should be clearly defined and assigned to various employees according to their skillset (Lobschat et al., 2021). In NFF, the division of labour creates control and combined action. This control is also monitored by the organisation by leveraging digital platforms and IT solutions (such as detective analytics) to monitor and track activities regarding financial transactions. This creates synergy in providing a holistic view of the different teams' efforts and activities conducted to trace, track, and prevent financial crime in a financial institution. This holistic view ensures that there are clearly defined roles and responsibilities from both the business and IT departments on how to prevent and mitigate intrusion from perpetrators of financial crimes.

7.3.2.4. Externalisation

Externalisation has been defined and referred to from various disciplines and perspectives such as business and political science (see Adams (1991), Marti (2013), Faist (2019), and Cobarrubias et al. (2023)). In the context of this study, externalisation is the process through which an organisation understands the construction of external reality and how it affects its internal operations. Kowalkowski et al. (2011) suggest that understanding externalisation is critical because of the many risks associated with external factors, which can constitute the main challenges of internalisation. The interpretation using AT is shown in Figure 7.2. In externalisation, various tools are used by actors (subjects) within departments or units (community) on the object of financial transaction or crime. Thus, externalisation has communication and intrusion attributes, as shown in Figure 7.4.

Tools: From the externalisation perspective, the utilisation of tools can contribute to positive or negative results for the organisation. The positive result of using tools is ensuring that the organisation has enough security protocols for their network and firewall which authenticates access to any confidential data (Yeboah-Boateng & Kwabena-Adade, 2020). However, as revealed from the data analysis, the negative utilisation of tools by perpetrators can yield an intrusion into the organisation's transaction data and processes. The tools provide ease of access and communication for perpetrators to commit financial crimes in NFF. Nikkel (2020) argues that perpetrators infiltrate the network to commit financial crimes using tools such as wireless remote access.

Subject and Community: The subject is an actor, which can be an employee or a perpetrator. The community members can be two groups; the employees of NFF and the perpetrators. According to Karanasios (2018), a community is a formation of a group or individuals that share the same interest through the object that interacts with the subject. In NFF, the employees of both the business and IT departments have roles to play in ensuring that perpetrators do not gain access to the confidential data or processes that can aid the committing of financial crimes. However, the same community can be infiltrated by a mole who is working with the perpetrators and providing them with confidential data and access to the applications and systems used by the organisation. Hashim et al. (2020) believe that regardless of their level in the organisation, any employee can commit financial crimes with perpetrators. Thus, it is critical to understand detective analytics, including the influencing factors, in applying the technology to mitigate financial crimes.

Object: In AT, an object is a thing that poses a problem or point of interest within an activity (Spinuzzi, 2011). Iyamu (2024) explains that without tools, subjects will not be able to achieve their objectives towards the object. The objective of the activity system is to prevent and mitigate financial crimes. However, in NFF the prevention and mitigation strategies have loopholes. For example, as revealed in the data analysis, anomalies within transactions are only discovered after the occurrence of the financial crime. Kurshan et al. (2020) state that the detection of financial crimes in organisations has not yet been mastered using current approaches and techniques. Hence, the perpetrators are still able to access and commit financial crimes within organisations. In applying detective analytics, an understanding of influencing factors and how they manifest, as presented in this study, is intended to bridge gaps and loopholes.

7.3.2.5. Digitalisation

Digitalisation entails the use of emerging technologies including the development of new and human-centric services (Redlein & Höhenberger, 2020). This means transforming from analogue to digital. In some organisations, digitalisation is a requirement for executing operational and strategic activities through technologies enabling digital formats (Voitsekh, 2022). In applying detective analytics, digitalisation is influenced by factors such as the corroborative effort of individuals and units, internalisation of processes and activities, and integration with other analytics tools as depicted in the Framework (Figure 7.4). Primarily, tools and rules are required to enforce digitalisation. Also, digitalisation can yield positive or negative results. This is to positively streamline the automation and synchronisation of applications and systems utilised. This was also revealed in NFF. The approach is intended to provide ease of use and access to the transactional data generated and stored by the organisation and its stakeholders. The negative impact is through digitalisation; perpetrators can easily find loopholes in accessing the transaction data.

Tools: The digitalisation of operations and activities within an organisation is not possible without using tools (Louw & Nieuwenhuizen, 2020). Due to digitisation, organisational activities and processes rely on data for processing millions of transactions daily (Hasan & Rizvi, 2022). In NFF, the tools used dominantly to trace, track, and prevent financial crime are data analytics tools. These tools enable the employees within the organisation to collaborate to ensure the prevention and mitigation of financial crimes. Digitalisation leverages internal processes and procedures to ensure that all requirements from both business and IT departments adhere to the outlined objective within the activity system.

Rules: The rules that govern digitalisation must meet both business and IT requirements to ensure the corroboration of information. Additionally, for any development and use of tools, rules need to be clearly defined and followed. In NFF, this is guided by the organisation's requirements which are leveraged from the internal policies and standards defined for preventing and mitigating financial crimes. Fernández-Macías (2018) argues that the automation of digitalisation in organisations is enforced by defined rules which guide the implementation and monitoring of the process.

7.3.2.6. Organisational structure

Organisational structure refers to the hierarchical setting through which processes and activities are structured and coordinated (Nwankwo et al., 2022). In the same vein, organisational structure guides the activities and processes conducted by NFF. From the mapping (Figure 7.3), the organisational structure has relationships with rules, subjects, community, and division of labour towards mitigating financial crimes in the organisation. Due to its critical role, organisational structure relies on rules to guide the employees (subjects) through various structures or units (community). Based on the guidance, roles and responsibilities (division of labour) are assigned. As shown in Figure 7.4, the organisational structure can influence internalisation and how analytics tools are integrated to create cohesiveness for deploying detective analytics.

Rules: From an AT perspective, rules are created to mediate how activities and processes should be conducted. As shown in the Framework (Figure 7.4), the organisational structure provides control for the internalisation of processes and activities. Thus, rules govern how detective analytics can be applied to mitigate financial crimes in an environment. Balcerek et al. (2021) contend that without rules, an organisation would not have governance over its operations, employees, and processes. In NFF, there were rules that both business and IT adhered to, to trace, track, and prevent financial crimes. What is even more important is how the rules are formulated and applied. Hassan and De Filippi (2021) argued that rules define coordination, collaboration, accountability, and clarity, to ensure and maintain consistency in the operations and objectives of the organisation.

Subject and community: The hierarchy outlines the subjects' activities, which are directed to an object (Carvalho et al., 2015). Subjects are members of a community, purposely to perform activities. The community forms part of the structures within an organisation. The community plays a very crucial role in shaping the organisational structure and creating a sense of belonging. Stewart and Townley (2020) emphasise that a community embodies the cultural norms, values, and practices that influence the employees' sense of belonging within the organisation. As revealed from the data analysis, both the business and IT departments have a collective identity and objective to prevent and mitigate financial crimes within the organisation. There is alignment between the community based on the rules that are defined within the organisational structure. The community creates ease of shared knowledge and skills which enable the employees within the different units to collaborate effectively and enhance their capabilities.

Division of labour: The organisational structure has a responsibility to clearly define the division of labour, to ease the execution of tasks in mitigating financial crimes. As shown in the Framework (Figure 7.4), the division of labour creates control to govern the internal processes. Consequently, the organisational structure ensures that the division of labour across the teams is fair and geared towards the organisation's objectives. As revealed from the data analysis, there are different units within the business and IT departments and within these units are teams which are grouped according to their skill sets. This ensures that each actor knows their roles and responsibilities in the activity system to prevent and mitigate financial crimes. Belbin and Brown (2022) state that division of labour aids the optimisation of organisational performance. In NFF, this also enables the control over the defined responsibilities, collaboration and innovation.

7.3.2.7. Integrated analytics

The use of multiple data analytics tools and methods is common in many organisations. This creates challenges and detrimental loopholes for the organisations. Thus, it is critical to integrate the analytics tools, as induced in Figure 7.4. The term 'integrated analytics' refers to the seamless use of various analytical tools such as descriptive, diagnostic, predictive, prescriptive and detective analytics (Schaefer & Makatsaria, 2021). An integrated analytics approach fortifies and heightens the sophistication of the analytics for mitigating financial crimes. In NFF, these data analytical tools are used to trace, track and prevent financial crimes. As revealed from the data analysis, there are loopholes with any technology use. These could be identified negatively by intruders who use analytical tools to defraud the organisation. Positively, NFF will now understand the importance of using integrated analytics to enhance its daily activities and operations to trace, track, and prevent financial crimes.

Rules: Rules in any technological advancement are needed for governance and control. Gupta et al. (2020) state that rules play a significant role in integrated analytics by shaping how activities are conducted and how data is interpreted. As revealed from the data analysis, the interpretation of data to trace, track, and prevent financial crime plays a huge role in the activity system. The data is used for decision-making and detecting any anomalies within the transactional activities. The NFF employs analytical tools such as SAS and OBIEE. These analytics tools must be integrated through configuration that is based on rules, which control how the tools should operate and what is important to identify within the data to trace, track, and prevent financial crimes. Duan and Da Xu (2021) argue that without rules, data analytics tools will not make meaningful connections and insights from the data. To adopt and use detective analytics, rules need to be defined for effective data decision-making, to mitigate anomalies.

Tools: Integrated analytics, in the context of this study, is the integration of detective analytics with other analytics, from prescriptive to diagnostic and predictive analytics. Also, Manoharan et al. (2023) described integrated analytics as the combination of various data sources, data analytics methods, and tools. As depicted in the Framework (Figure 7.4), on the one hand, integrated analytics is influenced by leverage and requirements, primarily. Firstly, it relies on the organisational structure to ensure there is leverage with the organisation's goals and objectives. Secondly, it considers digitalisation, for requirements that include technology and business solutions. In NFF, detective analytics can be deployed to trace, track, and prevent financial crime in a financial institution. On the other hand, the framework guides how integrated analytics can leverage the organisational structure to enhance the use of integrated analytical tools such as detective analytics. Mlambo and Iyamu (2024) argue that organisations should use detective analytics to trace and track perpetrators committing financial crimes.

Division of labour: Division of labour results in an output, positively or negatively (Karanasios, 2018). From the positive perspective, in mitigating financial crimes using detective analytics, the output is a result of a coordinated effort of labour and a group of labour. The negative result is the action of infiltrators. In NFF, it is revealed from the data analysis that there is a division of labour for preventing and mitigating financial crimes. Within the business and IT departments, several units use data analytics tools to enhance their operations and processes. Moreover, the different units specialise in different aspects and use several tools. This could be attributed to the fact that the different employees (actors) focus on different aspects such as data storage, analysis, interpretation, and visualisation. Such circumstance makes integrated analytics critical. One of the reasons is that it ensures enhanced expertise and improves the quality of data analysis to trace, track, and prevent financial crime. Levi and Soudijn (2020) agree that through data analytics, organisations make informed decisions based on the data.

7.4. Framework as an Instrumentation for Detective Analytics

The framework provides an instrumentation for detective analytics to mitigate financial crimes. The instrumentation is a two-step approach.

The first step helps to understand the relationships between the factors that influence mitigating financial crimes in an organisation. In interpreting the factors and their relationships, the attributes and their manifestations were revealed.

The second step presents the framework. As shown in Figure 7.4, a framework was developed. The framework is an instrumentation in that it provides a guide on why and how detective analytics can be applied in mitigating financial crimes in an organisation. This includes the following:

a. It reveals the factors that can influence detective analytics for mitigating financial crimes.

b. It reveals the roles of the factors and how they manifest, which entails the attributes.

c. It helps to understand how to employ the influencing factors to mitigate financial crimes in the organisation.

As an instrumentation, each component (factor) of the framework requires automation. The automation is defined by a template. Distinctively, each template provides guidelines on how to use detective analytics to mitigate financial crimes. The guidelines should focus on the operations of the organisation.

7.5. Summary

There is a gap and loophole in how the organisation is currently preventing and mitigating financial crimes. The Framework (Figure 7.4) unpacks the factors that organisations need to understand to adopt and implement detective analytics. As detailed in the interpretation of the findings above, organisations need to understand the seven factors that influence the use of detective analytics, including how they manifest, to prevent and mitigate financial crimes. The factors are as follows; (1) Collaboration; (2) Corroboration; (3) Internalisation; (4) Externalisation; (5) Digitalisation; (6) Organisational structure; and (7) Integrated analytics. The proposed framework (Figure 7.4) can be used to guide the adoption and implementation of detective analytics to trace, track, and prevent financial crimes in financial institutions in South Africa. The next chapter concludes the study.

CHAPTER EIGHT
CONCLUSION AND RECOMMENDATIONS

8.1. Introduction

This chapter presents the conclusion of the study. The study aimed to develop a tool that can be used to implement detective analytics to mitigate financial crimes. In achieving the study's aim, objectives were formulated as follows: (1) To understand the factors that influence financial crimes in South African financial institutions; thereafter, examine the current preventative and mitigative measures. (2) To investigate how the detective analytics tool can be deployed to trace, track, and prevent financial crime in a financial institution. (3) Based on objectives (1) and (2), an instrument was developed to define and enable the implementation and use of detective analytics to mitigate financial crimes. Moreover, in achieving the aim, appropriate methods, approaches, and techniques were employed.

For ease of flow, logic and understanding, the chapter is structured into eight sections. In the first section, the summary of the chapters is outlined, followed by the evaluation of the study in the second section. The third section summarises the outcome of the study. This is followed by the contribution of the research in the fourth section. The limitations of the study are outlined in section five, followed by the recommendations and further studies in sections six and seven. Finally, the conclusion is drawn in section eight.

8.2. Summary of the chapters

The study was rigorous and comprehensive. The problem was clearly articulated as presented in Chapter 1, based on which aligned objectives and questions were formulated. Two theories, activity theory (AT) and actor-network theory (ANT) add rigour to the study. The thesis is structured into eight chapters. This section provides the summary of each of the chapters, as follows:

Chapter 1 provides an overview of the whole study. A background of the research is provided to give context to how the study was formulated. The research problem is also presented to rationalise and support the background, providing context on the gap identified in the existing body of knowledge. The research objectives, questions and aim of the study are presented to understand what the study wants to achieve. The literature review section briefly outlines key focus areas of the study which are financial crimes in institutions, detective analytics and underpinning theories which are the Actor-network theory (ANT) and Activity theory (AT). This chapter also provides the methodology which outlines the philosophical assumption, research approach, methods, design, data collection and analysis. The rest of the chapter covered the ethical considerations, the significance of the research, the delineation, and the contribution of the study.

Chapter 2 presents an in-depth review of literature related to the core aspects of the study, which are financial crimes in organisations and detective analytics for financial crime. The key areas reviewed were financial crime, financial crime in organisations, the adoption of technology to mitigate financial crime and detective analytics for financial crime. The literature review chapter assisted in obtaining an in-depth knowledge of the phenomena and the gap identified from existing studies. This provides context to existing material to gain more knowledge on the use of detective analytics for preventing and mitigating financial crimes in organisations. At the time of the study, there was not much literature covered by other researchers in this area with a focus on using detective analytics. The Actor-network theory (ANT) and Activity theory (AT) theories underpinning this study were also reviewed, including their application in information systems studies.

The theoretical framework is outlined in Chapter 3. This chapter presents the order of using the ANT and AT theories to underpin the study. This provides context to how the two theories were used; the ANT to guide and underpin the data analysis of the study and the AT to guide the interpretation of the findings formulated in the data analysis. The chapter includes the advantages and disadvantages of the two theories. The chapter provides a critique of the use of ANT for this study and also justifies why the sociotechnical theory's strength impacts the study. The theoretical framework is developed and presented to clearly outline the order of use with the figure illustrating the order in which the two theories were used for the study.

The research methodology is presented in Chapter 4. In this chapter, the philosophical assumption, research approach, research method, research design, data collection process, data analysis process and the unit of analysis are provided. The selection of methods and approaches used for this study was guided by its aim, objectives and questions. This study used the qualitative method which guided and informed the design, being a case study and documentation of existing materials. Inductive reasoning was applied to gain more knowledge about the phenomena and to create themes and patterns of the data collected. Data was collected using semi-structured interviews and through a literature survey using document analysis (existing documents). This also outlines how the data was collected from database sources. The two keywords used to search for the papers were detective analytics and financial crime. The ethical implication, a brief discussion of the data analysis, and the unit of analysis are also presented.

Chapter 5 presents the overview of the data collection for this research. This provides an overview of the sources of data used for the study. The primary data for this study was obtained through conducting semi-structured interviews. The secondary data was collected through existing documents. The chapter provides a discussion on how the fieldwork was conducted in the organisation And, subsequently, how the existing data was collected and the credible sources used. The processes followed during the fieldwork and ethical considerations for both the organisation and the university are also discussed. The case selected for this study is one of South Africa's major financial institutions. A pseudo name, Nikiwe Federal Finance (NFF), was assigned to the organisation.

Chapter 6 presents the data analysis of the study guided by the actor-network theory's four moments of translation tenet. An overview of the data analysis is provided. The findings which are also referred to as factors from the data analysis are listed in this chapter. Seven factors were found to influence the use of detective analytics to mitigate financial crimes in organisations. The factors are as follows; (1) Collaboration; (2) Corroboration; (3) Internalisation; (4) Externalisation; (5) Digitalisation; (6) Organisational structure; and (7) Integrated analytics. Also revealed from the analysis is the fundamental relationship between the seven factors.

The interpretation of the findings is presented in Chapter 7. The findings were interpreted using the activity theory (AT). This means that a mapping of the factors (factors from analysis) with AT components was created. Based on the mapping, the influencing factors are linked and attributes are established through subjectivism. The AT components are used to examine the factors including their attributes. The chapter outlines how the interpretation of the findings followed two steps. The two steps were followed to gain insights into the relationship between the factors that influence the mitigation of financial crimes in an institution and to develop a framework that guides an understanding of how detective analytics can be deployed to trace, track, and prevent financial crime in a financial institution. Based on the influencing factors, a framework was developed. The framework depicts the links and dependence between the factors. The framework is a tool that can be used to implement detective analytics to mitigate financial crimes.

Chapter 8 concludes the entire study by revisiting its objectives and summarising how they were met. It outlines the theoretical, practical, and methodological contributions made. Additionally, this chapter addresses the study's limitations and offers recommendations.

8.3. Evaluation of the research

The evaluation of any research is a very critical process that is conducted for several reasons, including assessing the validity, credibility and reliability of the research (Wanzer, 2021). The evaluation, according to Iyamu and Shaanika (2019), is conducted using 6 components referred to as the 5Ws and 1H (what, where, who, when, why, and how). These components guide the identification of limitations, considerations for future research, enhancing transparency and contributions of the study to the existing body of knowledge. Table 8.1 presents the evaluation.

Table 8.1: Evaluation of the study

Component	Evaluation of the study
What	The implementation of detective analytics to mitigate financial crime in organisations was investigated from the context of South Africa. The study entails two main aspects which are financial crimes and the use of detective analysis, as explained in chapters 2 and 5 respectively. Based on the focus of the study, the problem was articulated from a South African perspective. The problem helps to form the research objectives and questions presented in Chapter 1 and revisited in Chapter 4. Data was collected focusing on understanding the nature of financial crimes perpetrated in South African financial institutions, followed by an examination of the current preventative and mitigative measures and how the detective analytics tool can be deployed to trace, track, and prevent financial crime in a financial institution. The data was analysed in Chapter 6 and findings were obtained. The interpretation of findings to examine the integration aspect of the study was presented in Chapter 7.
Where	As consistently stated in the thesis, the research was conducted in South Africa. One financial institution, Nikiwe Federal Finance (NFF), was involved in the study. NFF is a pseudonym, as explained in Chapter 4. The organisation is one of the largest financial institutions in South Africa. The rationale for selecting the organisation including the ethics followed is also discussed in Chapter 4. The organisation is structured into 2 departments, namely, business and IT. This was also supported by obtaining academic papers from credible sources (databases). The focus areas were crime in financial institutions and detective analytics. This process supports the credibility and usefulness of the research in guiding further inquiry.
Who	In achieving the objectives or answering the research questions, individuals and groups were selected to participate in the study. The criteria used in selecting the individuals are discussed in Chapter 4. Chapter 5 presents the demographics of the groups (departments and units). Different perspectives and points of view were obtained from both the business and IT departments. From the business department, the participants were from different units; the compliance and enforcement unit (CEU), financial surveillance (FinServ), risk management unit (RMU), prudential authority (PAU), and the money laundering unit (MLU). The participants from the IT department were selected from the business solutions, data analysts, IT security, and machine-learning units. All the participants were from the senior management level. Furthermore, existing material focussing on financial crimes, and detective analytics were used.. The data was collected using a set of criteria that included the areas of focus, detective analytics, publication timeframe, and credible sources.
When	The study was conducted within three years. It was started in 2021 by following the University (CPUT) processes including the development and approval of the research proposal. Thereafter, organisations were contacted and selected, and data collection began. The data collection was carried out from 12 June 2024 to 31 July 2024. The study reached a point of saturation after 12 interviews were conducted. The data analysis began in August 2024 and concluded in October 2024. This was to prevent any delays in data collection as any change could have occurred during that time in the field of financial crimes and detective analytics. That could have affected the reliability and quality of the research.
Why	Primarily, the research was conducted for two reasons. Firstly, financial crimes are increasing in South Africa and many parts of the world. This research intended to contribute to reducing financial crimes in organisations. Secondly, detective analytics could be used more effectively for understanding and mitigating financial crimes. However, many organisations do not understand the factors that influence the implementation of detective analytics.

	From the literature review, there is currently a gap and loophole in how organisations prevent and mitigate financial crimes. There is currently no framework that can be used to implement and use detective analytics to mitigate financial crimes. Also, the study gives an understanding of the factors and attributes that need to be considered when implementing and using this framework.
How	The study applied the interpretive paradigm and adopted an inductive approach. It adopted the qualitative method and implemented a case study design. Data was gathered through semi-structured interviews and analysis of existing documents. Two theories, Actor-Network theory (ANT) and Activity theory (AT) were used to underpin the study. This means that the ANT was used as a lens to guide the data analysis and AT to interpret the findings from the analysis. Based on the interpretation, an instrument was developed to define and enable the implementation and use of detective analytics to mitigate financial crimes.

8.4. Summary of the outcomes

The research aimed to develop a tool that can be used to implement detective analytics to mitigate financial crimes. In achieving the aim of the research, three objectives were formulated. How the objectives were achieved is discussed below.

i. **The first objective is to understand the factors that influence financial crimes that happen in South African financial institutions and, thereafter, examine the current preventative and mitigative measures.**

This objective was achieved from the comprehensiveness of the data analysis as presented in Chapter 6, which helps to gain a deeper understanding of the nature of financial crimes committed in South African institutions. This includes identifying all the actor networks and the various actors involved in the processes and activities used to prevent and mitigate financial crimes. This was presented in subsection 6.3.1, Chapter 6.

The study used ANT to first understand the actors involved either internally or externally. The internal actors are from both the business and IT departments. In the two departments, various units are involved in ensuring that adequate measures are in place to prevent and mitigate financial crimes. These units have built a comprehensive framework for preventing and mitigating financial crimes in NFF. The external actors are different stakeholders that have an interest in the operations of the organisation. Moreover, the perpetrators also act as stakeholders in NFF due to their interest in committing financial crimes. Thus, the preventive and mitigative measures in NFF are not operating as intended.

In the business department, the organisation has introduced and implemented various policies and standards that govern how financial crimes should be prevented and mitigated in NFF. The IT department has also implemented these policies and standards in configuring their applications and systems. The rules and configurations that these applications and systems follow are defined within the financial crimes framework that both the business and IT departments adhere to. However, as revealed from the data analysis in Chapter 6, there is a gap and loophole in how the organisation is currently preventing and mitigating financial crimes. This could be attributed to multiple factors.

However, as noted in NFF, all applications and systems used to trace, track, and prevent financial crime only discover the anomalies post-occurrence of the incidents, which means there is no detective measure or control to detect and disclose them. Therefore, there is a need for NFF to adopt and implement detective analytics.

ii. To investigate how the detective analytics tool can be deployed to trace, track, and prevent financial crime in a financial institution.

In achieving this objective, data relating to detective analytics were collected from the organisation that participated in the study and literature. Thereafter, an analysis was conducted. From the analysis, a two-step procedure was followed to investigate how the detective analytics tool can be deployed to trace, track and prevent financial crime in NFF.

In the first step, the relationships between the factors (findings) were established, as shown in Figure 7.3. The relationships help to understand how the factors can influence the deployment of detective analytics in an organisation. Also, the relationships draw on both technical and non-technical influences. The first step is critical because it establishes the foundation towards mitigating financial crimes.

In the second step, meanings were associated with the factors. From the analysis presented in Chapter 6, 7 factors were revealed. As illustrated in Chapter 7, Figure 7.4., this was conducted to understand how financial crimes happen in the organisation. The factors were examined using AT. This was done because of two reasons. Firstly, the influencing factors have a relationship between them as they do not operate in silos. Secondly, AT components are mapped with the influencing factors.

iii. Based on objectives i and ii, an instrumentation will be developed, to define and enable the implementation and use of detective analytics, to mitigate financial crimes.

The above objectives revealed seven factors: (1) Collaboration; (2) Corroboration; (3) Internalisation; (4) Externalisation; (5) Digitalisation; (6) Organisational structure; and (7) Integrated analytics. Based on the influencing factors, a framework is developed, as shown in Chapter 7 (Figure 7.4), the Framework depicts the links and dependence between the factors. Arrows are used to illustrate links and dependence between these factors. Also, the influence of the factors is facilitated by various attributes. These attributes include communication, control, requirements, synergy, leverage, and intrusion. The attributes were revealed in the data analysis.

Section 7.4 of Chapter 7 explains how the Framework is or can be used as an instrument for implementing detective analytics in an organisation. This includes recommendations for developing templates through which the influencing factors towards mitigating financial crimes in an organisation can be detailed.

8.5. Contribution of the Research

The research contributes to academics and society, including business and government. The contributions of the research are viewed from three perspectives: theoretical, methodological, and practical.

8.5.1 Theoretical contribution

Theoretically, the study contributes from three standpoints. First, it contributes by revealing the seven factors that were found to influence the use of detective analytics to mitigate financial crimes. Based on these factors, the actors involved in mitigating financial crimes can better understand why certain things happen in the ways that they do.

Secondly, the framework is a major contribution to the body of knowledge for two reasons. Firstly, it revealed how the influencing factors and the attributes linking them are connected. Secondly, it provides a compendium of how the influencing factors can be deployed to guide the implementation of detective analytics to prevent and mitigate financial crimes. As of the time of this study, such a framework was non-existent. Moreover, no framework within the financial crime domain focuses on the use of detective analytics.

Thirdly, it adds to the existing literature in the fields of information systems, finance, and detective analytics. Currently, as shown in Chapter 2, the literature on detective analytics is scanty. There are limited academic studies on the subject of detective analytics. Also, it is a significant contribution from a developing country’s perspective, especially South Africa, as the study was conducted in that context.

8.5.2. Methodological contribution

The complementary use of the actor-network theory (ANT) and activity theory (AT) to guide the data analysis and interpretation of findings, respectively, is a methodological contribution. It advances the complementarity of sociotechnical theories in IT studies. This is the first evidence in academic databases of combining both theories in a study in the areas of financial crimes and detective analytics.

Also, how ANT and AT were used in this study is unique, as depicted in Figure 3.3 which shows the order of use for the two theories. Iyamu (2024) argues that there exist challenges in attempts to complementarily use sociotechnical theories in IS research. ANT was first used to identify human and non-human actors, including the actor networks that existed in preventing and mitigating financial crimes in a financial institution. Then, the activities were interpreted using AT through the six components: subject, tool, object, rules, community and division of labour.

8.5.3. Practical contribution

Practically, the framework can be used as a guide to trace, track, and monitor financial transactions in an organisation. This can be done by following the actors (Latour, 2005) to gain insights into the traces of the processes of financial transactions and actions of the intruders. The framework induces a method into business and IT processes for mitigating financial crime in an organisation. Currently, it is difficult to find a framework that can be used to guide the implementation of detective analytics to detect financial crimes.

The practical contribution is very important to the South African context. This is particularly so because there is currently a gap and loophole in how the organisation prevents and mitigates financial crimes. Thus, the framework is critical in ensuring and enabling financial institutions in South Africa to trace, track, and prevent financial crimes. Also, the study offers a better understanding of the factors that influence the use of detective analytics to mitigate financial crimes in organisations.

8.6. Limitations of the study

Primarily, three limitations were identified for this study:

i. The study focuses on the use of detective analytics specifically from a South African financial institution perspective. This means that the study does not include all developing countries and is primarily focused on the South African context. However, the study can be applied in other financial institutions in developing countries that utilise detective analytics as a mechanism for detecting financial crime.

ii. The study did not include the technological tools used by intruders as a part of its investigation.

iii. The data analytics family has other tools such as descriptive analytics, diagnostic analytics, predictive analytics, and prescriptive analytics. However, for this study, only detective analytics was used as a tool to detect financial crimes as and when they happen.

8.7. Recommendations

To implement the framework proposed in the study, the following recommendations are made: Integration of analytics tools, integration of detective analytics with other systems and processes, development of a template for each factor, and training.

8.7.1. Integration of analytics tools

The integration of analytics tools such as detective analytics, descriptive analytics, diagnostic analytics, predictive analytics, and prescriptive analytics aids the ability to gather insights, monitor, trace and track (Menezes et al., 2019). Organisations can leverage integrating their analytics tools to make informed decisions. However, it is critical to understand the abilities of these analytical tools to ensure that the various selected tools achieve the objectives of the organisation. Sreemathy et al. (2020) state that the integration enables data collection from various applications and systems within the organisation. Therefore, the data integration layer needs to be well-defined to extract, transform and load (ETL) processes from these different sources. Furthermore, controls need to be in place to ensure compliance and security between the different layers of the integration process.

8.7.2 Integration of detective analytics with other systems and processes

The integration of detective analytics with other systems and processes will enhance organisations' ability to detect anomalies, trace, track and monitor potential threats (Martínez-Fernández et al., 2018). However, for the integration to be successful, the objectives of using detective analytics for the different use cases must be clearly defined (Delgado et al., 2021). This will ensure that the organisation can track the effectiveness of using detective analytics for the various use cases. Moreover, Loshin (2013) argues that for the integration to be a success, data aggregation needs to be clearly defined to understand the different data sources and what the detective analytics tool needs from these sources to operate as intended.

8.7.3. Development of a template for each factor

Templates provide a structure that guides the process of integrating detective analytics using different factors (Bloomfield et al., 2021). This also enhances the collaboration and quality through the process followed by the organisation. The development of a template for each factor in the integration of detective analytics with other systems and processes assists in creating a standard approach and ensures a thorough coverage of each aspect. The purpose of developing a template for each factor is to clearly define the objectives of the detective analytics integration and how they will be achieved based on the defined templates. Developing a template ensures that processes and documentation are done consistently across all different use cases.

8.7.4. Training

Some financial institutions have the skills to enhance their data analytics capabilities. However, the gap of not being able to detect anomalies as and when they occur needs to be covered by implementing detective analytics. Both the business and IT departments' employees need to be part of the process to develop and implement a new solution using the proposed framework in Figure 7.4. Therefore, personnel at all levels should be trained on how to apply detective analytics.

8.8. Further Study

The aim and objectives of the research were achieved as documented in chapters 6 and 7 and highlighted in this chapter. However, some areas could be further studied to enhance and expand the topic as an academic stream. The proposed areas include a research stream, the IT solutions used in committing financial crimes and testing the framework as a research stream in IT solutions and data analytics usage. The researcher suggests further study in the area of testing the framework in financial institutions and analysing the results. This type of research can be conducted following the quantitative paradigm.

8.9. Conclusion

This chapter outlines the research conclusions and recommendations. The research was assessed in relation to the objectives established in Chapter 1, which were revisited in the concluding chapter to confirm that all objectives were met. The chapter also discussed the research's theoretical, methodological, and practical contributions of the study, as well as its limitations and suggestions for future research. A framework was developed to define and enable the implementation and use of detective analytics to mitigate financial crimes.

REFERENCES

Abdallah, A., Maarof, M.A. & Zainal, A. 2016. Fraud detection system: A survey. *Journal of Network and Computer Applications*, 68:90-113.

Abusharbeh, M., 2024. The influence of knowledge creation process on customer relations management: evidence from Palestinian commercial banks. *EuroMed Journal of Business*, 19(3):684-702.

Achim, M.V., Borlea, S.N. & Văidean, V.L. 2021. Does technology matter for combating economic and financial crime? A panel data study. *Technological and Economic Development of Economy*, 27(1):223-261.

Adams, K. 1991. Externalisation vs specialisation: what is happening to personnel? *Human Resource Management Journal*, 1(4):40-54.

Adeoye-Olatunde, O.A. and Olenik, N.L., 2021. Research and scholarly methods: Semi-structured interviews. *Journal of the American college of Clinical Pharmacy*, 4(10):358-1367.

Adhabi, E. and Anozie, C.B., 2017. Literature review for the type of interview in qualitative research. *International Journal of Education*, 9(3):86-97.

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. 2020. Analysis of cyber-crime effects on the banking sector using the balanced scorecard: A survey of literature. *Journal of Financial Crime*, 27(3):945-958.

Akinbowale, O.E., Klingelhöfer, H.E. & Zerihun, M.F. 2024. Investigating the level of effectiveness of the anti-fraud technologies employed by the South African banking industry for cyberfraud mitigation. *Journal of Financial Crime*, 31(1):201-225.

Al-Najran, N. & Dahanayake, A. 2015. A requirements specification framework for big data collection and capture. In *New Trends in Databases and Information Systems: ADBIS 2015 Short Papers and Workshops*, *BigDap, DCSA, GID, MEBIS, OAIS, SW4CH, WISARD,* Poitiers, France, 8-11 September*. Proceedings*. Springer International Publishing.

Albrecht, W.S., Albrecht, C.O., Albrecht, C.C. & Zimbelman, M.F. 2019. *Fraud examination*. 6th Edition, Cengage Learning, Boston, MA.

Alexander, P. M. & Silvis, E. 2014. Towards extending actor-network theory with a graphical syntax for information systems research. *Information Research,* 19(2) paper 617. [Available at http://InformationR.net/ir/19-2/paper617.html].

Aliguliyev, R., Imamverdiyev, Y. & Abdullayeva, F. 2016. The investigation of opportunities of big data analytics as analytics-as-a-service in cloud computing for oil and gas industry. *Problems of Information Technology*, 7(1):9-22.

Alisherovich, T.S. And Ugli, N.B.B., 2023. Internal Control In Banks. *European journal of business startups and open society*, 3(3):34-39.

Almakhfor, R.A. & Norton, S.D. 2021. Audit committees in financial institutions in Saudi Arabia: A dichotomy of perceptions of functional independence and the reporting of financial crime. *Journal of Financial Crime*, 28(4):1065-1077.

Alsghaier, H., Akour, M., Shehabat, I. & Aldiabat, S. 2017. The importance of big data analytics in business: A case study. *American Journal of Software Engineering and Applications*, 6(4):111-115.

Amara, I. & Khlif, H. 2018. Financial crime, corruption and tax evasion: A cross-country investigation. *Journal of Money Laundering Control*, 21(4):545-554.

Amer, T. B., & Al-Omar, M. I. A. 2023. The impact of cyber security on preventing and mitigating electronic crimes in the Jordanian banking sector. *International Journal of Advanced Computer Science and Applications*, 14(8):371-380.

Andriosopoulos, D., Doumpos, M., Pardalos, P.M. and Zopounidis, C., 2019. Computational approaches and data analytics in financial services: A literature review. *Journal of the Operational Research Society*, 70(10):1581-1599.

Apuke, O.D. 2017. Quantitative research methods: A synopsis approach. *Kuwait Chapter of Arabian Journal of Business and Management Review*, 33(5471):1-8.

Apuke, O.D. 2017. Quantitative research methods a synopsis approach. *Arabian Journal of Business and Management Review (Kuwait Chapter)*, 6(11):40-47.

Ara, A., Maraj, M.A.A., Rahman, M.A. & Bari, M.H. 2024. The impact of machine learning on prescriptive analytics for optimized business decision-making. *International Journal of Management Information Systems and Data Science*, 1(1):7-18.

Avis, J. (2009) Transformation or transformism: Engeström's version of activity theory? *Educational review (Birmingham)*. 61(2):151–165.

Avortri, C. & Agbanyo, R. 2020. Determinants of management fraud in the banking sector of Ghana: The perspective of the diamond fraud theory. *Journal of Financial Crime*, 28(1):142-155.

Azungah, T., 2018. Qualitative research: deductive and inductive approaches to data analysis. *Qualitative research journal*, 18(4):383-400.

Baiocchi, G., Graizbord, D. and Rodríguez-Muñiz, M., 2013. Actor-Network Theory and the ethnographic imagination: An exercise in translation. *Qualitative Sociology*, 36:323-341.

Balaji, E., Brindha, D. & Balakrishnan, R. 2020. Supervised machine learning-based gait classification system for early detection and stage classification of Parkinson's disease. *Applied Soft Computing*, 94:106494.

Balcerek, S., Karovič, V. and Karovič, V. 2021. Application of Business Rules Mechanism in IT System Projects. *Developments in Information & Knowledge Management for Business Applications:* 2:33-112.

Baloyi, X.N., 2020. The influence of smart technologies within service-oriented organisations. Doctoral dissertation, Cape Peninsula University of Technology.

Barab, S., Schatz, S. & Scheckler, R. 2004. Using activity theory to conceptualize online community and using online community to conceptualize activity theory. *Mind, Culture, and Activity*, 11(1):25-47.

Bargoni, A., Ferraris, A., Vilamová, Š., & Wan Hussain, W. M. H. 2024. Digitalisation and internationalisation in SMEs: a systematic review and research agenda. *Journal of Enterprise Information Management*, 37(5):1418-1457.

Bataev, A.V. 2018, September. Evaluation of using big data technologies in Russian financial institutions. In 2018 *IEEE International Conference" Quality Management, Transport and Information Security, Information Technologies"(IT&QM&IS)*. St. Petersburg, Russia, 24-28 September. IEEE.

Bazen, A., Barg, F.K. and Takeshita, J., 2021. Research techniques made simple: an introduction to qualitative research. *Journal of Investigative Dermatology*, 141(2):241-247.

Bedny, G.Z., Seglin, M.H. and Meister, D., 2000. Activity theory: history, research and application. *Theoretical issues in ergonomics science*, 1(2):168-206.

Behfar, K. and Okhuysen, G.A., 2018. Perspective—Discovery within validation logic: Deliberately surfacing, complementing, and substituting abductive reasoning in hypothetico-deductive inquiry. *Organization Science*, 29(2):323-340.

Belbin, R.M. and Brown, V., 2022. *Team roles at work*. Routledge.

Benson, A., Lawler, C. and Whitworth, A., 2008. Rules, roles and tools: Activity theory and the comparative study of e-learning. British Journal of Educational Technology, 39(3):456-467.

Bergman, M.M. & Coxon, A.P. 2005. The quality in qualitative methods. In *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research* 6(2):1-23.

Bertelsen, O.W. and Bødker, S. 2003. Activity theory. *HCI Models, Theories, and Frameworks: Toward a Multidisciplinary Science*, 291-324.

Bloomfield, R., Fletcher, G., Khlaaf, H., Hinde, L. and Ryan, P., 2021. Safety case templates for autonomous systems. *arXiv preprint arXiv:2102.02625*, 1-135.

Bos-Nehles, A., Bondarouk, T. and Labrenz, S., 2017. HRM implementation in multinational companies: The dynamics of multifaceted scenarios. *European Journal of International Management*, 11(5):515-536.

Bowron, M. & Shaw, O. 2007. Fighting financial crime: A UK perspective. *Economic Affairs*, 27(1):6-9.

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007). Lessons from applying the systematic literature review process within the software engineering domain. *Journal of systems and software*, 80(4):571-583.

Broeders, D., Schrijvers, E., van der Sloot, B., Van Brakel, R., de Hoog, J. & Ballin, E.H. 2017. Big data and security policies: towards a framework for regulating the phases of analytics and use of Big Data. *Computer Law & Security Review*, 33(3):309-323.

Brown, P. 2017. Narrative: an ontology, epistemology and methodology for pro-environmental psychology research. *Energy Research & Social Science*, 31:215-222.

Bryman, A., 2016. *Social research methods*. Oxford University Press.

Bueger, C. and Stockbruegger, J., 2017. Actor-network theory: objects and actants, networks and narratives. In *Technology and world politics* (pp. 42-59). Routledge.

Buqa, A. & Fung, C.N. 2019. Scoping digital business strategy in banking: A comparative study of Italy, Sweden and Switzerland. Master's thesis, University of Gothenburg.

Callon, M., 1984. Some elements of a sociology of translation: domestication of the scallops and the fishermen of St Brieuc Bay. *The sociological review*, 32(1):196-233.

Callon, M., 1986. The sociology of an actor-network: The case of the electric vehicle. In *Mapping the dynamics of science and technology: Sociology of Science in the real world* (pp. 19-34). London: Palgrave Macmillan UK.

Carvalho, M.B., Bellotti, F., Berta, R., De Gloria, A., Sedano, C.I., Hauge, J.B., Hu, J. and Rauterberg, M., 2015. An activity theory-based model for serious games analysis and conceptual design. *Computers & education*, 87:166-181.

Chapter, A.O.T., 2004. 5 qualitative analysis of experience: grounded theory and case studies. *Research methods for clinical and health psychology*, 69.

Chauhan, R.S., 2022. Unstructured interviews: are they really all that bad?. *Human Resource Development International*, 25(4):474-487.

Cheng, X., Liu, S., Sun, X., Wang, Z., Zhou, H., Shao, Y. & Shen, H. 2021. Combating emerging financial risks in the big data era: A perspective review. *Fundamental Research*, 1(5):595-606.

Chitimira, H. & Ncube, M. 2020. Legislative and other selected challenges affecting financial inclusion for the poor and low-income earners in South Africa. *Journal of African Law*, 64(3):337-355.

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. *Potchefstroom Electronic Law Journal (PELJ),* 24(1):1-33.

Chivanga, S.Y. and Monyai, P.B., 2021. Back to basics: Qualitative research methodology for beginners. *Journal of Critical Reviews*, 8(2):11-17.

Choi, S., Kim, S., Kwon, S., & Shin, J. Y. (2021). Analyst forecasts and target setting in executive annual bonus contracts. *Journal of Management Accounting Research*, 33(2):19-42.

Choto, T., 2018. *Cyber financial crimes: detection, prevention, investigation & reporting*, Macroeconomic and Financial Management Institute of Eastern and Southern Africa. Zimbabwe. Retrieved from https://coilink.org/20.500.12592/vn272p on 03 Nov 2024. COI: 20.500.12592/vn272p.

Clarke, E., 2021. Methodological Pragmatism--Freedom from the Squeeze?. *International Journal of Multiple Research Approaches*, 13(3).

Coats, A. 1983. Subjectivism. In *Beyond Positive Economics? Proceedings of Section F (Economics) of the British Association for the Advancement of Science York 1981*, 87.

Cobarrubias, S., Cuttitta, P., Casas-Cortés, M., Lemberg-Pedersen, M., El Qadim, N., İşleyen, B., ... & Heller, C. (2023). Interventions on the concept of externalisation in migration and border studies. *Political geography*, 105(3):102911.

Cockcroft, S. & Russell, M. 2018. Big data opportunities for accounting and finance practice and research. *Australian Accounting Review*, 28(3):323-333.

Coetzee, J. 2018. Strategic implications of Fintech on South African retail banks. *South African Journal of Economic and Management Sciences*, 21(1):1-11.

Collins, P., Shukla, S. and Redmiles, D. 2002. Activity theory and system design: A view from the trenches. *Computer Supported Cooperative Work (CSCW)*, 11:55-80.

Contreras, S. & Ghosh, A. 2022. COVID-19 and its impact on minority-owned banks. In *AEA Papers and Proceedings*(Vol. 112, pp. 313-318). American Economic Association.

Cook, N. 2020. South Africa: Current issues, economy, and US relations. available at: https://sgp.fas.org/ crs/row/R45687.pdf (Access 14 May 2024).

Couldry, N., 2008. *Actor-network theory and media: Do they connect and on what terms*? In: Hepp, Andreas, Krotz, Friedrich, Moores, Shaun and Winter, Carsten, (eds.) Connectivity, Networks and Flows: Conceptualizing Contemporary Communications. Hampton Publishing, Cresskill, NJ, USA, 93-110. ISBN 9781572738577.

Crang, M. 2003. Qualitative methods: touchy, feely, look-see? *Progress in Human Geography*, 27(4):494-504.

Crawford, T.H., 2020. Actor-network theory. *In Oxford research encyclopedia of literature.* Oxford University Press. https://doi.org/10.1093/acrefore/9780190201098.013.965

Dagada, R. 2024. The advancement of 4IR technologies and increasing cyberattacks in South Africa. *Southern African Journal of Security*,27.

De Jesus Liriano EDD, R., 2019. Improving the Learning Process in the Higher Education Through the Use of a Predictive Tool (Dashboard). *FDLA Journal*, 4(1):7.

De Koker, L. & Goldbarsht, D. 2022. Financial technologies and financial crime: Key developments and areas for future research. In *Financial Technology and the Law: Combating Financial Crime* (pp. 303-320). Cham: Springer International Publishing.

De Koker, L. 2007. Financial crime in South Africa. *Economic Affairs*, 27(1):34-38.

Delgado, Y., Price, B.S., Speaker, P.J. and Stoiloff, S.L., 2021. Forensic intelligence: Data analytics as the bridge between forensic science and investigation. *Forensic Science International: Synergy*, 3;100162.

Derindere Köseoğlu, S., Ead, W.M. & Abbassy, M.M. 2022. Basics of financial data analytics. In *Financial Data Analytics: Theory and Application* (pp. 23-57). Cham: Springer International Publishing.

Deshpande, P.S., Sharma, S.C., Peddoju, S.K., Deshpande, P.S., Sharma, S.C. & Peddoju, S.K. 2019. A network-based intrusion detection system. *Security and Data Storage Aspect in Cloud Computing*,35-48.

Diremelo, T.M. 2020. The tension between bank secrecy and the combating of financial crime*.* Doctoral dissertation, University of Pretoria.

Dolwick, J.S., 2009. 'The social'and beyond: Introducing actor-network theory. *Journal of maritime archaeology*, 4:21-49.

Donning, H.A.N.N.A., Eriksson, M.A.T.H.I.A.S., Martikainen, M.I.N.N.A. & Lehner, O.M. 2019. Prevention and detection for risk and fraud in the digital age–the current situation. *ACRN Oxford Journal of Finance and Risk Perspectives*, 8:86-97.

Doolin, B. and Lowe, A., 2002. To reveal is to critique: actor–network theory and critical information systems research. *Journal of information technology*, 17:69-78.

Dowsley, F. 2021. National Centre for Crime and Justice Statistics, Australia. *The Encyclopedia of Research Methods in Criminology and Criminal Justice*, 1:81-87.

Duan, L. and Da Xu, L., 2021. Data analytics in industry 4.0: A survey. *Information Systems Frontiers*,1-17.

Dubovsky, S.L. 2024. Will Interviewing Become a Lost Art?. *Psychotherapy and Psychosomatics*, 93(2):75-79.

Dunn, M., Nel, V., van den Berg, H.S. and Huyssteen, E., 2023. The application of constructivist grounded theory methodology in an urban planning doctoral thesis. International Journal of Qualitative Methods, 22:1-10.

Ebneyamini, S. and Sadeghi Moghadam, M.R., 2018. Toward developing a framework for conducting case study research. International journal of qualitative methods, 17(1):1-11.

Ehiane, S.O., Olofinbiyi, S.A. and Mkhize, S.M. eds., 2023. *Cybercrime and Challenges in South Africa*. Palgrave Macmillan.

El Mouaaouy, F. 2018. Financial crime 'hot spots'– empirical evidence from the foreign exchange market. *The European Journal of Finance*, 24(7-8):565-583.

Empl, P. & Pernul, G. 2023. Digital-twin-based security analytics for the Internet of Things. *Information*, 14(2):95.

Endjala, T. 2022. An Employee Assistance Programme (EAP) to support midwives affected by maternal deaths and stillbirths in Khomas region, Namibia. Doctoral dissertation, University of Namibia.

Engeström, Y. 1999. Activity theory and individual and social transformation. *Perspectives on activity theory*, 19(38):19-30.

Engeström, Y., Miettinen, R. and Punamäki-Gitai, R.L. eds., 1999. *Perspectives on activity theory*. Cambridge University Press.

Engestrom, Y., 2000. Activity theory as a framework for analyzing and redesigning work. Ergonomics, 43(7):960-974.

Engeström, Y. 2001. Expansive learning at work: Toward an activity theoretical reconceptualization. *Journal of Education and Work*, 14(1):133-156.

Engeström, Y., 2009. The future of activity theory: A rough draft. Learning and expanding with activity theory,303-328.

Ericson, J. 2021. Communication Breakdown: identifying weaknesses and improvement possibilities in the cooperation between law enforcement and financial institutions regarding romance fraud. Dissertation, Malmö University.

Ettema, D. 2018. Apps, activities and travel: A conceptual exploration based on activity theory. *Transportation*, 45(2):273-290.

Faist, T. 2019. Contested externalisation: responses to global inequalities. *Comparative Migration Studies*, 7(1),1-8.

Faried, M.E.D., 2018. The influence of the critical diffusion factors of 3D printing technology on the success of UAE construction Projects. Master's thesis, The British University in Dubai.

Fernández-Macías, E. 2018. Automation, digitalisation and platforms: Implications for work and employment. Eurofound Working Paper.

Ferreira, E. & Koko, K. 2022. Latest crime statistics: Murder, kidnapping and commercial crimes increase. Available; https://mg.co.za/news/2022-02-18-latest-crime-statistics-murder-kidnapping-and-commercial-crimes-increase/. Date accessed 28 March 2023.

Fontana, M., Peverelli, F. and Giacomazzi, M., 2022. Collaboration in East Africa: A contextual definition. *Education Sciences*, 12(10),:706.

Fossey, E., Harvey, C., McDermott, F. and Davidson, L., 2002. Understanding and evaluating qualitative research. *Australian & New Zealand Journal of psychiatry*, 36(6):717-732.

Fosso Wamba, P.S. 2017. Big data analytics and business process innovation. *Business Process Management Journal*, 23(3):470-476.

Frizzo-Barker, J., Chow-White, P.A., Adams, P.R., Mentanko, J., Ha, D. & Green, S. 2020. Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management*, 51:1-14.

Futerman, R. G. 2015. Design for collaboration in South Africa : an activity theory perspective on participatory design. Cape Peninsula University of Technology.

Ganesan, A., Parameshwarappa, P., Peshave, A., Chen, Z. and Oates, T., 2019. Extending signature-based intrusion detection systems withbayesian abductive reasoning. *arXiv preprint arXiv:1903.12101*, 1-10.

Gao, P. 2005. Using actor-network theory to analyse strategy formulation. *Information Systems Journal*, 15(3):255-275.

Gaumer, Q., Mortier, S. & Moutaib, A. 2016. Financial institutions and cyber crime: Between vulnerability and security. *FSR FINANCIAL*, 45.

Gerrard, Y. 2021. What's in a (pseudo) name? Ethical conundrums for the principles of anonymisation in social media research. *Qualitative Research*, 21(5):686-702.

Gerring, J. 2017. Qualitative methods. *Annual review of political science*, 20:15-36.

Giddens, A. 1984. *The constitution of society: Outline of the theory of structuration*. Cambridge: Polity Press.

Giebe, C., Hammerström, L. & Zwerenz, D. 2019. Big data & analytics as a sustainable customer loyalty instrument in banking and finance. *Financial Markets, Institutions and Risks*, 3(4):74-88.

Gilchrist, D. 2022. Taking an intelligence-led approach: How to improve understanding of financial crime threats through intelligence and analysis. *Journal of Financial Compliance*, 5(4):315-323.

Glass, R. L., Ramesh, V., & Vessey, I. 2004. An analysis of research in computing disciplines. *Communications of the ACM*, 47(6):89-94.

Gombiro, C., Jantjies, M. & Mavetera, N. 2015. A conceptual framework for detecting financial crime in mobile money transactions. *Journal of Governance and Regulation,* 4(4):727-734.

Greulich, M., Lins, S., & Sunyaev, A. 2020. Toward Uncovering Patterns of Certification Internalization. In *ICIS*, 1-8.

Gupta, A., 2024. Types of Data, Data Collection, and Storage Methods. In *Qualitative Methods and Data Analysis Using ATLAS. ti: A Comprehensive Researchers' Manual* (pp. 31-59). Cham: Springer International Publishing.

Gupta, S., Leszkiewicz, A., Kumar, V., Bijmolt, T. and Potapov, D., 2020. Digital analytics: Modeling for insights and new methods. *Journal of Interactive Marketing*, 51(1):26-43.

Hájek, A. & Hartmann, S. 2010. Bayesian epistemology, 93-105.

Harwalkar, S.S., Hussein, A.H.A., Kumar, B.V., Habelalmateen, M.I. and Victoria, R.M., 2023, November. Intrusion Detection in IoT Platform Using Tuna Swarm Optimization with Long Short-Term Memory. In *2023 International Conference on Ambient Intelligence, Knowledge Informatics and Industrial Electronics (AIKIIE)* (pp. 1-6). IEEE.

Hasan, H. & Pfaff, C. C. 2012. An activity theory analysis of corporate wikis. *Information Technology & People*, 25(4):423-437.

Hasan, I., & Rizvi, S. A. M. 2022. AI-driven fraud detection and mitigation in e-commerce transactions. In *Proceedings of Data Analytics and Management: ICDAM 2021, Volume 1* (pp. 403-414). Springer Singapore.

Hasham, S., Joshi, S. & Mikkelsen, D. 2019. Financial crime and fraud in the age of cybersecurity. *McKinsey & Company*, *2019*, 1-11.

Hashim, H.A., Salleh, Z., Shuhaimi, I. and Ismail, N.A.N., 2020. The risk of financial fraud: a management perspective. *Journal of Financial Crime*, *27*(4):1143-1159.

Haslam, S.A., Reicher, S.D. and Platow, M.J., 2020. The new psychology of leadership: Identity, influence and power. Routledge, London.

Hassan, S. and De Filippi, P., 2021. Decentralized autonomous organization. *Internet Policy Review*, *10*(2).

Hayati, N. and Dalimunthe, I.S., 2022. Integration of Science Based on Philosophy Review (Study Aspects of Ontology, Epistemology, and Axiology). *ITQAN: Jurnal Ilmu-ilmu Kependidikan*, *13*(2):169-182.

Heeks, R., & Stanforth, C. 2015. Technological change in developing countries: Opening the black box of process using actor–network theory. *Development Studies Research*, 2(1):33-50.

Hellstrand, A. & Breckwoldt, M. 2016. *Consumer acceptance of mobile banking in Germany*, 1-16. Thesis, Jonkoping University.

Hoa, C.T.H., 2024. Action Research. In Applied Linguistics and Language Education Research Methods: Fundamentals and Innovations (pp. 164-181). IGI Global.

Hoelscher, J.L. & Shonhiwa, T. 2021. Not so fuzzy auditing analytics. *Journal of Emerging Technologies in Accounting*, *18*(1):99-112.

Holcombe, R. G. 2018. Checks and balances: enforcing constitutional constraints. *Economies*, 6(4), 57.

Hollweck, T. 2015. Case Study Research Design and Methods . Thousand Oaks, CA: Sage. 282 pages. *Canadian Journal of Program Evaluation*, 30(1).

Holt, T.J., Bossler, A.M. & Seigfried-Spellar, K.C. 2022. *Cybercrime and digital forensics: An introduction*. Routledge, London.

Holzenthal, F. 2017. Five trends shaping the fight against financial crime. *Computer Fraud & Security*, 2017(3):5-9.

Hope Sr, K.R. 2020. Channels of corruption in Africa: Analytical review of trends in financial crimes. *Journal of Financial Crime*, 27(1):294-306.

Hsbollah, H.M., Simon, A. and Letch, N., 2016. Understanding the Implementation of IT Governance Arrangements and IT Infrastructure Using Actor Network Theory. *International Journal of Actor-Network Theory and Technological Innovation (IJANTTI)*, 8(2):44-55.

Hussain, M., Nadeem, M.W., Iqbal, S., Mehrban, S., Fatima, S.N., Hakeem, O. & Mustafa, G. 2021. Security and privacy in FinTech: A policy enforcement framework. In *Research Anthology on Concepts, Applications, and Challenges of FinTech* (pp. 372-384). IGI Global.

Ifenthaler, D. 2017. Designing effective digital learning environments: Toward learning analytics design. *Technology, Knowledge and Learning*, 22:401-404.

Indergård, K., 2022. Interdisciplinarity in light of Actor-Network Theory. In *Proceedings of the 3rd Transdisciplinary Workplace Research Conference 7-10 September 2022 in Milan, Italy: TWR NETWORK*. Politecnico di Milano Milan, Italy.

Islam, M. 2020. Data Analysis: Types, Process, Methods, Techniques and Tools. *International Journal on Data Science and Technology*, 6(10).

Islam, M.R., Liu, S., Biddle, R., Razzak, I., Wang, X., Tilocca, P. and Xu, G., 2021. Discovering dynamic adverse behavior of policyholders in the life insurance industry. *Technological Forecasting and Social Change*, *163*:1-14.

Ivanyuk, V. 2023. Forecasting of digital financial crimes in Russia based on machine learning methods. *Journal of Computer Virology and Hacking Techniques*,1-14.

Iyamu, T. 2020. A Case for Applying Activity Theory to IS Research. *Information resources management journal*. [Online] 33 (1);1–15.

Iyamu, T. 2024. The Application of Sociotechnical Theories in Information Systems Research. London: Cambridge Scholars Publishing.

Iyamu, T. & Shaanika, I. 2019. The use of activity theory to guide information systems research. *Education and Information Technologies*, 24(1):165-180.

Iyamu, T. 2018. Collecting qualitative data for information systems studies: The reality in practice. *Education and Information Technologies*, 23*:* 2249-2264.

Iyamu, T. 2020. A case for applying Activity Theory in IS research. *Information Resources Management Journal (IRMJ)*, 33(1):1-15.

Iyamu, T. 2021. *Applying theories for information systems research*. Routledge, London.

Iyamu, T. and Ibitomi, R.A., 2024. A Model for Supporting Information Technology Solutions Selection and Evaluation in a Nigerian Bank. *Journal of Logistics and service science,* 11(4):351-366.

Iyamu, T. and Shaanika, I., 2019. The use of activity theory to guide information systems research. *Education and Information Technologies*, 24:165-180.

Iyamu, T., 2020. A case for applying Activity Theory in IS research. *Information Resources Management Journal (IRMJ)*, 33(1):1-15.

Iyamu, T., Nehemia-Maletzky, M., & Shaanika, I. 2016. The overlapping nature of business analysis and business architecture: What we need to know. *Electronic Journal of Information Systems Evaluation*, 19(3):169-179.

Janakiraman, S. & Ayyanathan, N., 2021. *Big Data Framework for Indian Green Coffee Export Demand Modeling and Descriptive Analysis using Nosql-MONGODB* (No. 6919). EasyChair.

Jasinski, D., Phillips, A. & Johnston, E. eds. 2023. *Organised Crime, Financial Crime, and Criminal Justice: Theoretical Concepts and Challenges*. Taylor & Francis, Routledge, New York.

Jeble, S., Dubey, R., Childe, S.J., Papadopoulos, T., Roubaud, D. & Prakash, A. 2018. Impact of big data and predictive analytics capability on supply chain sustainability. *The International Journal of Logistics Management*, *29*(2):513-538.

Johnson, O. and Iyamu, T., 2019. Framework for the adoption of e-commerce: A case of South African retail grocery sector. *The Electronic Journal of Information Systems in Developing Countries*, 85(5):1-12.

Jonassen, D.H. and Rohrer-Murphy, L., 1999. Activity theory as a framework for designing constructivist learning environments. Educational technology research and development, 47(1):61-79.

Kammerer, Y., Gottschling, S., & Bråten, I. 2021. The role of internet-specific justification beliefs in source evaluation and corroboration during web search on an unsettled socio-scientific issue. *Journal of Educational Computing Research*, 59(2):342-378.

Kaptelinin, V. & Miettinen, R. 2005. Introduction: "Perspectives on the Object of Activity". *Mind, Culture, and Activity*, 12(1):1-3.

Kaptelinin, V. & Nardi, B. 2018. Activity theory as a framework for human-technology interaction research. *Mind, Culture, and Activity*, 25(1):3-5.

Karanasios, S. 2014. Framing ICT4D Research Using Activity Theory: A Match Between the ICT4D Field and Theory? *Information technologies and international development*. 10 (2):1–17.

Karanasios, S. 2018. Toward a unified view of technology and activity: The contribution of activity theory to information systems research. *Information Technology & People*, *31*(1):134-155

Karanasios, S. & Allen, D. 2018 Activity theory in Information Systems Research. *Information systems journal (Oxford, England)*. [Online] 28 (3):439–441.

Karanasios, S., Allen, D.K. & Finnegan, P. 2018. Activity theory in Information Systems Research. *Inf. Syst. J.,* 28(3):439-441.

Kaur, S., Kaur, G., Sodhi, G.S. and Kaur, J., 2023. Forensic importance of toolmarks evidence: A review. *International Journal of Medical Toxicology & Legal Medicine*, *26*(1and2): 110-114.

Kempen, A. 2020. The world of private investigators in South Africa. *Servamus Community-based Safety and Security Magazine*, *113*(11):34-37.

Khedr, A., Kholeif, S. & Saad, F. 2017. An integrated business intelligence framework for healthcare analytics. *International Journal*, *7*(5).

Khotsa, K.C. 2019. The effects of crime in the South African Post Office: A case of the North East Region. *International Conference on Public Administration and Development Alternatives* (IPADA). 03 - 05 July, Southern Sun Hotel, OR Tambo International Airport, Johannesburg, South Africa.

Kiili, C., Bråten, I., Kullberg, N., & Leppänen, P. H. 2020. Investigating elementary school students' text-based argumentation with multiple online information resources. *Computers & Education*, *147*, 103785.

Kirby, K. and Anwar, M.N., 2020. An application of activity theory to the "problem of e-books". *Heliyon*, *6*(9):1-19.

Klecuń, E., 2004. Conducting critical research in information systems: can actor-network theory help?. *Information systems research: Relevant theory and informed practice*, 259-274.

Kolli, S. and Khajeheian, D., 2020. How actors of social networks affect differently on the others? Addressing the critique of equal importance on actor-network theory by use of social network analysis. *Contemporary applications of actor network theory*, 211-230.

Koskosas, I.V., 2008. Trust and risk communication in setting Internet banking security goals. *Risk Management*, 10:56-75.

Koval, V., Nazarova, K., Hordopolov, V., Kopotiienko, T., Miniailo, V. & Diachenko, Y. 2019. Audit in the state economic security system. *Management Theory and Studies for Rural Business and Infrastructure Development*, *41*(3):419-430.

Kowalkowski, C., Kindström, D., & Witell, L. (2011). Internalisation or externalisation? Examining organisational arrangements for industrial services. *Managing Service Quality: An International Journal*, *21*(4):373-391.

Kshetri, N. 2019. Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, 22(2):77-81.

Kumar, V., & Tissenbaum, M. 2022. Supporting collaborative classroom networks through technology: An actor network theory approach to understanding social behaviours and design. *British Journal of Educational Technology*, 53(6):1549-1570.

Kurshan, E., Shen, H. and Yu, H., 2020, September. Financial crime & fraud detection using graph computing: Application considerations & outlook. In *2020 Second International Conference on Transdisciplinary AI (TransAI)* (pp. 125-130). IEEE.

Kute, D.V., Pradhan, B., Shukla, N. & Alamri, A. 2021. Deep learning and explainable artificial intelligence techniques applied for detecting money laundering–a critical review. *IEEE Access*, 9:82300-82317.

Lacity, M., Willcocks, L., & Gozman, D. (2021). Influencing information systems practice: The action principles approach applied to robotic process and cognitive automation. *Journal of Information Technology*, *36*(3):216-240.

Latour, B. 1996. On actor-network theory: A few clarifications. *Soziale welt*, 369-381.

Latour, B., 2005. An introduction to actor-network-theory. *Reassembling the social*. Oxford University Press.

Latour, B., 2007. *Reassembling the social: An introduction to actor-network-theory*. Oxford University Press.

Latour, B., 2017. On actor-network theory. A few clarifications plus more than a few complications. *Philosophical Literary Journal Logos*, *27*(1):173-197.

Lazarova-Molnar, S., Mohamed, N. & Al-Jaroodi, J. 2018. Collaborative data analytics for industry 4.0: Challenges, opportunities and models. In *2018 Sixth International Conference on Enterprise Systems (ES),* 01-02 October, Limassol, Cyprus (pp. 100-107). IEEE.

Lee, A.S. and Liebenau, J., 1997, January. Information systems and qualitative research. *In Information Systems and Qualitative Research: Proceedings of the IFIP TC8 WG 8.2 International Conference on Information Systems and Qualitative Research*, 31st May–3rd June 1997, Philadelphia, Pennsylvania, USA (pp. 1-8). Boston, MA: Springer US.

Lee, C.S., Cheang, P.Y.S. & Moslehpour, M. 2022. Predictive analytics in business analytics: Decision tree. *Advances in Decision Sciences*, *26*(1):1-29.

Lefkowitz, D. 2022. Black boxes and information pathways: An actor-network theory approach to breast cancer survivorship care. *Social Science & Medicine*, 307:115184.

Levi, M. and Soudijn, M., 2020. Understanding the laundering of organized crime money. *Crime and Justice*, *49*(1):579-631.

Lezaun, J. 2017. Actor-network theory. In *Social theory now* (eds) C. Benzecry, M. Krause & I. Reed, 305-31. Chicago: University Press.

Li, J., Li, J., Zhu, X., Yao, Y., & Casu, B. 2020. Risk spillovers between FinTech and traditional financial institutions: Evidence from the US. *International Review of Financial Analysis*, 71:101544.

Liu, X., Shin, H., & Burns, A. C. 2021. Examining the impact of luxury brand's social media marketing on customer engagement: Using big data analytics and natural language processing. *Journal of Business Research*, 125:815-826.

Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M. and Wirtz, J., 2021. Corporate digital responsibility. *Journal of Business Research*, 122:pp.875-888.

Loke, M.H., Rucker, D.F., Chambers, J.E., Wilkinson, P.B. and Kuras, O., 2021. Electrical resistivity surveys and data interpretation. In *Encyclopedia of solid earth geophysics* (pp. 344-350). Cham: Springer International Publishing.

López-Robles, J.R., Rodríguez-Salvador, M., Gamboa-Rosales, N.K., Ramirez-Rosales, S. & Cobo, M.J. 2019. The last five years of big data research in Economics, Econometrics and Finance: Identification and conceptual analysis. *Procedia Computer Science*, *162*: 729-736.

Loshin, D., 2013. *Big data analytics: from strategic planning to enterprise integration with tools, techniques, NoSQL, and graph*. Elsevier.

Louw, C. and Nieuwenhuizen, C., 2020. Digitalisation strategies in a South African banking context: A consumer services analysis. *South African Journal of Information Management*, *22*(1):1-8.

Lundh, L.G., 2020. Experimental phenomenology in mindfulness research. Mindfulness, 11(2): 493-506.

Macdonald, D. 2019. Barriers to reconstruction and development: A brief view of corruption and economic crime in Southern Africa. In *Structural Adjustment, Reconstruction and Development in Africa* (pp. 172-178). Routledge.

Magaldi, D. & Berler, M. 2020. Semi-structured interviews. *Encyclopedia of Personality and Individual Differences*, 4825-4830.

Manoharan, S.G.S., Subramaniam, R. and Mohapatra, S., 2023. Strategic Decision-Making Through Integrated Data Analytics. In *Enabling Strategic Decision-Making in Organizations Through Dataplex* (pp. 65-75). Emerald Publishing Limited.

Marelino, A. 2022. Understanding the types of cybercrime and its prevention. *Mathematical Statistician and Engineering Applications*, 71(1):108-112.

Marti, E. (2013). Mechanisms of internalisation and externalisation of knowledge in Piaget's and Vygotsky's theories 1. In *Piaget Vygotsky* (pp. 57-83). Psychology Press.

Martínez-Fernández, S., Jovanovic, P., Franch, X. and Jedlitschka, A., 2018, August. Towards automated data integration in software analytics. In *Proceedings of the International Workshop on Real-Time Business Intelligence and Analytics,*1-5.

Marxen, K. 2022. When context matters - application and potential of financial crime risk indicators in selected African jurisdictions. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, *25*(1):1-22.

Mazhar, S.A., Anjum, R., Anwar, A.I. and Khan, A.A., 2021. Methods of data collection: A fundamental tool of research. *Journal of Integrated Community Health (ISSN 2319-9113)*, *10*(1):6-10.

Mazorodze, B.T. 2020. Youth unemployment and murder crimes in KwaZulu-Natal, South Africa. *Cogent Economics & Finance*, *8*(1):1-17.

McCusker, K. & Gunaydin, S. 2015. Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion*, 30(7):537-542.

McKee, H. 2017. An Instructor Learning Analytics Implementation Model. *Online Learning*, 21(3):87-102.

Menezes, B.C., Kelly, J.D., Leal, A.G. & Le Roux, G.C. 2019. Predictive, prescriptive and detective analytics for smart manufacturing in the information age. *IFAC-PapersOnLine*, 52(1):568-573.

Mentari, N., & Hudi, N. (2022). Prevention of Financial Crime after Covid 19. In *Ahmad Dahlan International Conference on Law and Social Justice* (pp. 85-102): UAD Press.

Merlonghi, G. 2010. Fighting financial crime in the age of electronic money: Opportunities and limitations. *Journal of Money Laundering Control*, *13*(3):202-214.

Mfinanga, F.A., Mrosso, R.M. and Bishibura, S., 2019. Comparing case study and grounded theory as qualitative research approaches. *Focus*, *2*(05):51-56.

Michael, M. 2016. Actor-network theory: *Trials, trails and translations*. Sage Publications.

Mitchell, A. and Education, A.E., 2018, July. A Review of Mixed Methods, Pragmatism and Abduction Techniques. *The Electronic Journal of Business Research Methods*, 16(3):103-116.

Mlambo, N. and Iyamu, T., 2024. Conceptualising the use of detective analytics underpinned by Actor-network theory. *Issues in Information Systems*, *25*(1):419-433.

Monteiro, S. and Kahlke, R., 2022. 1-1 The Philosophy of Science. *Health Professions Education Research Primer*.

Morgan, H. 2022. Conducting a qualitative document analysis. *The Qualitative Report*, 27(1): 64-77.

Moser, A. and Korstjens, I., 2018. Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *European journal of general practice*, *24*(1): 9-18.

Moser, A. and Korstjens, I., 2018. Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. European journal of general practice, 24(1): 9-18.

Muñoz, C., Galvez, D., Enjolras, M., Camargo, M. and Alfaro, M., 2022. Relationship between innovation and exports in enterprises: A support tool for synergistic improvement plans. *Technological Forecasting and Social Change*, 177:121489.

Murphy, A., Robu, K. & Steinert, M. 2020. The investigator-centered approach to financial crime: Doing what matters. *McKinsey and Company*,1-11.

Murphy, E. and Rodriguez-Manzanares, M.A., 2008. Using activity theory and its principle of contradictions to guide research in educational technology. *Australasian Journal of Educational Technology*, *24*(4).

Nakajima, C. 2007. Issues in fighting financial crime. *Economic Affairs*, 27(1):2-5.

Nangin, M.A., Barus, I.R.G. & Wahyoedi, S. 2020. The effects of perceived ease of use, security, and promotion on trust and its implications on fintech adoption. *Journal of Consumer Sciences*, *5*(2):124-138.

Nardi, B.A. 1996. Activity theory and human-computer interaction. *Context and Consciousness: Activity Theory and Human-Computer Interaction*, 436:7-16.

Nardi, B.A., 1996. Activity theory and human-computer interaction. *Context and consciousness: Activity theory and human-computer interaction*, *436*:7-16.

Nehemia-Maletzky, M., Iyamu, T. and Shaanika, I., 2018. The use of activity theory and actor network theory as lenses to underpin information systems studies. *Journal of Systems and Information Technology*, *20*(2):191-206.

Neuhaus, F. 2017. On the Definition of 'Ontology'. In *JOWO*. Available online: https://www.researchgate.net/profile/Fabian-Neuhaus-2/publication/323684434_On_the_Definition_of_'Ontology'/links/5aa3fbb90f7e9badd9a99d1e/On-the-Definition-of-Ontology.pdf (accessed on 31 January 2022).

Nguyen, T., Novak, R., Xiao, L. and Lee, J., 2021. Dataset distillation with infinitely wide convolutional networks. *Advances in Neural Information Processing Systems*, *34*:5186-5198.

Nguyen, T.H., Pham, X.L. & TU, N.T.T. 2021. The Impact of Design Thinking on Problem Solving and Teamwork Mindset in A Flipped Classroom. *Eurasian Journal of Educational Research*, *96*:30–50.

Nicholls, J., Kuppa, A. & Le-Khac, N.A. 2021. Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *IEEE Access*, 9:163965-163986.

Nikkel, B., 2020. Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation*, *33*:200908.

Nobanee, H. 2021. A bibliometric review of big data in finance. *Big Data*, *9*(2):73-78.

Northcote, M.T., 2012, April. Selecting criteria to evaluate qualitative research. This conference paper was originally published as: Northcote, M.(2012). Selecting criteria to evaluate qualitative research. In M. Kiley (Ed.), Narratives of Transition: Perspectives of Research Leaders, Educators & Postgraduates. Paper presented at the 10th Quality in Postgraduate Research Conference, Stamford Grand, Adelaide, 17-20 April (pp. 99-110). Canberra, Australia: The Centre for Higher Education, Learning and Teaching. The Australian National University. Retrieved from http://www. qpr. edu. au/wp-content/uploads/2015/09/QPR_2012_proceedings-1. pdf. ISBN: 9780646579573.

Nwankwo, C.A., Kanyangale, M.I. and Eze, S.U., 2022. Organisational Structure as a Strategic Enabler of Commercial Bank Employees in Nigeria. *Academic Journal of Interdisciplinary Studies*, 11(3):335-349.

Nyikana, W. and Iyamu, T., 2023. The logical differentiation between small data and big data. *South African Journal of Information Management*, *25*(1):1-9.

Nyikana, W., & Iyamu, T. 2023. A formulaic approach for selecting big data analytics tools for organizational purposes. In *Handbook of research on driving socioeconomic development with big data* (pp. 224-242). IGI Global.

Oakley, A., 1997. Epistemological problems of human agency in Mises's subjectivism. *History of Economics Review*, 26(1):21-39.

Osman, S., Mohammad, S., Abu, M.S., Mokhtar, M., Ahmad, J., Ismail, N. and Jambari, H., 2018. Inductive, Deductive and abductive approaches in generating new ideas: A modified grounded theory study. *Advanced Science Letters*, 24(4):2378-2381.

Othman, R., Laswad, F. & Berkahn, M. 2023. Financial crimes in small businesses: causes and consequences. *Journal of Financial Crime*, 30(3);742-758.

Patel, R., Migliavacca, M. & Oriani, M.E. 2022. Blockchain in banking and finance: A bibliometric review. *Research in International Business and Finance*, *62*:101718.

Peim, N., 2009. Activity theory and ontology. Educational Review, 61(2):167-180.

Pillai, M.M. and Helberg, A., 2021, September. Improving Security in Smart Home Networks through user-defined device interaction rules. In *2021 IEEE AFRICON,* 13-15 September, Arusha, Tanzania (pp. 1-6). IEEE.

Poli, R. & Seibt, J. eds. 2010. *Theory and applications of ontology: Philosophical perspectives*. New York: Springer.

Powelson, K. 2022. *The* Impact of Artificial Intelligence on Anti-money Laundering Programs to Detect and Prevent Financial Crime. Doctoral dissertation, Utica University, New York.

Pramanik, M.I., Lau, R.Y. & Chowdhury, M.K.H. 2016. Automatic crime detector: A framework for criminal pattern detection in big data era, https://aisel.aisel.org/pacis2016/311/.

Pramanik, M.I., Lau, R.Y., Yue, W.T., Ye, Y. & Li, C. 2017. Big data analytics for security and criminal investigations. *Wiley Interdisciplinary Reviews: Data Mining And Knowledge Discovery*, *7*(4):1208.

Qu, S.Q. & Dumay, J. 2011. The qualitative research interview. *Qualitative Research in Accounting & Management*, 8(3):238-264.

Raeesi Vanani, I. & Majidian, S. 2021. Prescriptive analytics in Internet of Things with concentration on deep learning. *Introduction to Internet of Things in Management Science and Operations Research: Implemented Studies*,31-54.

Raeithel, A., 1992. Activity theory as a foundation for design. In *Software development and reality construction* (pp. 391-415). Berlin, Heidelberg: Springer Berlin Heidelberg.

Ranjan, J. & Jeyanthi, M. 2021. Big Data Analytics in the Healthcare Industry. In *Global Business Leadership Development for the Fourth Industrial Revolution* (pp. 134-154). IGI Global.

Ravi, V. & Kamaruddin, S. 2017. Big data analytics enabled smart financial services: opportunities and challenges. In *Big Data Analytics: 5th International Conference,* BDA 2017, Hyderabad, India, December 12-15, 2017, Proceedings 5 (pp. 15-39). Springer International Publishing.

Redlein, A., & Höhenberger, C. 2020. Digitalisation. *Modern Facility and Workplace Management: Processes, Implementation and Digitalisation*, 139-175.

Rezigalla, A.A., 2020. Observational study designs: Synopsis for selecting an appropriate study design. *Cureus*, *12*(1).

Ridder, H.G., 2017. The theory contribution of case study research designs. Business research, 10:281-305.

Rouhollahi, Z. 2021. Towards artificial intelligence-enabled financial crime detection. *arXiv preprint arXiv*:2105.10866.

Runkler, T.A. 2020. *Data analytics*. Wiesbaden: Springer Fachmedien Wiesbaden, 26(4):1-22.

Saddiq, S.A. & Abu Bakar, A.S. 2019. Impact of economic and financial crimes on economic growth in emerging and developing countries: A systematic review. *Journal of Financial Crime*, *26*(3):910-920.

Sage, D., Dainty, A. & Brookes, N. 2011. How actor-network theories can help in understanding project complexities. *International Journal of Managing Projects in Business*, , *4*(2):274-293.

Sage, D., Vitry, C. and Dainty, A., 2020. Exploring the organizational proliferation of new technologies: An affective actor-network theory. *Organization Studies*, *41*(3):345-363.

Sahar, S.M., Safie, N. & Bakar, K.A.A. 2019. The challenges in managing information technology shared services operations. *International Journal of Recent Technology and Engineering*, 8:322-328.

Samuel, J. 2017. Information token-driven machine learning for electronic markets: Performance effects in behavioral financial big data analytics. *JISTEM-Journal of Information Systems and Technology Management*, *14*:371-383.

Sandhya, S. And Sujitha, K., 2022. A Study of Talent Management and Its Impact on Performance of Organizations, *international journal of innovative technologies,*10(2):89-93.

Sartania, T., 2021. Modern practice of leadership: Its role and importance in the successful operation of the organization. Globalization and Business, 6(12):162-165.

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.K.R. & Burnap, P. 2020. Impact and key challenges of insider threats on organizations and critical businesses. *Electronics*, *9*(9): 1460.

Sayes, E., 2014. Actor–Network Theory and methodology: Just what does it mean to say that nonhumans have agency?. *Social studies of science*, *44*(1):134-149.

Schaefer, C. and Makatsaria, A., 2021. Framework of data analytics and integrating knowledge management. *International Journal of Intelligent Networks*, *2*:156-165.

Scharrer, E. and Ramasubramanian, S., 2021. *Quantitative research methods in communication: The power of numbers for social justice*. Routledge, New York.

Scott, B.F. 2020. Red teaming financial crime risks in the banking sector. *Journal of Financial Crime*, *28*(1):98-111.

Sekgweleo, T. and Iyamu, T., 2022. Understanding the factors that influence software testing through moments of translation. *Journal of Systems and Information Technology*, *24*(3):202-220.

Selvan, C. & Balasundaram, S.R. 2021. Data analysis in context-based statistical modeling in predictive analytics. In *Handbook of Research on Engineering, Business, and Healthcare Applications of Data Science and Analytics* (pp. 96-114). IGI Global.

Sert, D. and Alparslan, Ş., 2022. Externalising externalisation and bad governance of migration in the EU: Turkey learning from Europe. In *EU Good Governance Promotion in the Age of Democratic Decline* (pp. 71-87). Cham: Springer International Publishing.

Setiawan, A. and Syamsuddin, D., 2022. Multidimensional Science Paradigm in the Philosophy Integration of Ontology, Epistemology, and Axiology. *Multidisciplinary International Journal of Research and Development*, 1(3):1-10.

Shim, Y. & Shin, D.H. 2016. Analyzing China's fintech industry from the perspective of actor–network theory. *Telecommunications Policy*, 40(2-3):168-181.

Sibanda, J., 2022. *Investigating the changing role of key performance indicators for technology and project management entities*. Doctoral dissertation, North-West University, South Africa.

Siemonova, B., 2017. Transactive memory system and Web 2.0 in knowledge sharing: A conceptual model based on activity theory and critical realism. *Information System Journal* 28(4):592-611

Sigetova, K., Uzikova, L., Dotsenko, T. & Boyko, A. 2022. Recent trends in the financial crime of the world. *Financial & Credit Activity: Problems of Theory & Practice*, 5(46).

Simanjuntak, E. and Hendriani, W., 2022. Using ethnography in psychological research: Challenges and opportunities. Using Ethnography in Psychological Research: Challenges and Opportunities, 30(1):45-58.

Singh, K. & Best, P. 2019. Anti-money laundering: Using data visualization to identify suspicious activity. *International Journal of Accounting Information Systems*, 34: 100418.

Siregar, S.A., Siregar, G. & Lubis, M.A. 2020. Criminological Perspective of street crime. *Journal of Advanced Research in Dynamical and Control Systems-JARDCS*, *12*(6):603-611.

Smith, T. 2020. Is the case study the evidence-base's equivalent to the dodo?. *The Knee*, 27(4):A1-A2.

Sofaer, S. 1999. Qualitative methods: What are they and why use them? *Health Services Research*, 34(5 Pt 2):1101.

Spinuzzi, C. 2011. Losing by expanding: corralling the runaway object. *Journal of Business and Technical Communication, 25(4)*:449-486.

Sreemathy, J., Nisha, S. and RM, G.P., 2020, March. Data integration in ETL using TALEND. In *2020 6th international conference on advanced computing and communication systems (ICACCS),*06-07 March, Coimbatore, India, (pp. 1444-1448). IEEE.

Steen, J., Coopmans, C. and Whyte, J., 2006. Structure and agency? Actor-network theory and strategic organization. *Strategic organization*, *4*(3):303-312.

Stewart, K. and Townley, G., 2020. How far have we come? An integrative review of the current literature on sense of community and well-being. *American Journal of Community Psychology*, *66*(1-2):166-189.

Subedi, K.R., 2021. Determining the Sample in Qualitative Research. Online Submission, 4:1-13.

Sukirman & Kabilan, M. K. 2023. Indonesian researchers' scholarly publishing: an activity theory perspective. *Higher education research and development*. [Online] 42(8):2030–2047.

Sukmawati, S., 2023. Development of quality instruments and data collection techniques. *Jurnal Pendidikan Dan Pengajaran Guru Sekolah Dasar (JPPGuseda)*, 6(1):119-124.

Sun, S., Huang, D. & Gong, Y. 2011. Gross error detection and data reconciliation using historical data. *Procedia Engineering*, 15:55-59.

Sun, Y., Shi, Y. & Zhang, Z. 2019. Finance big data: Management, analysis, and applications. *International Journal of Electronic Commerce*, 23(1):9-11.

Sunio, V. & Mendejar, J. 2022. Financing low-carbon transport transition in the Philippines: Mapping financing sources, gaps and directionality of innovation. *Transportation Research Interdisciplinary Perspectives*, *14*:100590.

Supriyanto, S., Meliala, A.E. & Sulhin, I. 2023. The dynamics of criminogenic organizational within the financial crime in Indonesia. *International Journal of Educational Research and Social Sciences (IJERSC)*, 4(3):508-523.

Suryani, A. 2008. Comparing case study and ethnography as qualitative research approaches. *Jurnal Ilmu Komunikasi*, 5(1):117-127.

Suryono, R.R., Budi, I. & Purwandari, B. 2020. Challenges and trends of financial technology (Fintech): A systematic literature review. *Information*, 11(12):590.

Sutherland, E. 2017. Governance of cybersecurity - the case of South Africa. *The African Journal of Information and Communication*, 20:83-112.

Sutrisno, A., Anggreni, L. and Prastyaningtyas, S.W., 2021. The influence of motivation and collaboration on organizational performance. *Turkish Online Journal of Qualitative Inquiry*, *12*(6).

Suzumura, T., Zhou, Y., Baracaldo, N., Ye, G., Houck, K., Kawahara, R., Anwar, A., Stavarache, L.L., Watanabe, Y., Loyola, P. & Klyashtorny, D. 2019. Towards federated graph learning for collaborative financial crimes detection. *arXiv preprint arXiv*:1909.12946.

Taherdoost, H., 2021. Data collection methods and tools for research; a step-by-step guide to choose data collection technique for academic and business research projects. International Journal of Academic Research in Management (IJARM), 10(1):10-38.

Tansu, G. 2023. Understanding the human factor in financial crime compliance. *Journal of Financial Compliance*, *6*(4):368-384.

Taquette, S.R. and Borges da Matta Souza, L.M., 2022. Ethical dilemmas in qualitative research: A critical literature review. International Journal of Qualitative Methods, 21, p.16094069221078731.

Tatnall, A., 2003. Actor-network theory as a socio-technical approach to information systems research. In *Socio-technical and human cognition elements of information systems* (pp. 266-283). Igi Global.

Teichmann, F.M.J. & Falker, M.C. 2021. Cryptocurrencies and financial crime: Solutions from Liechtenstein. *Journal of Money Laundering Control*, *24*(4):775-788.

Tessier, V. and Zahedi, M., 2022. Activity theory as a framework for understanding framing complexity of design projects, in Lockton, D., Lenzi, S., Hekkert, P., Oak, A., Sádaba, J., Lloyd, P. (eds.), DRS2022: Bilbao, 25 June-3 July, Bilbao, Spain. https://doi.org/10.21606/drs.2022.444

Thomas, D.R. 2006. A general inductive approach for analyzing qualitative evaluation data. *American Journal of Evaluation*, 27(2):237-246.

Thornton, D., Mueller, R.M., Schoutsen, P. & Van Hillegersberg, J. 2013. Predicting healthcare fraud in medicaid: a multidimensional data model and analysis techniques for fraud detection. *Procedia Technology*, 9:1252-1264.

Titchen, A. & Ajjawi, R. 2010. Writing contemporary ontological and epistemological questions about practice. In *Researching Practice*, 45-55, Brill.

Tolmen, R. 2020. Understanding the influence of technological innovation within the insurance industry in KwaZulu-Natal, Masters' Thesis, University of Kwazulu-Natal.

Trozze, A., Kamps, J., Akartuna, E.A., Hetzel, F.J., Kleinberg, B., Davies, T. & Johnson, S.D. 2022. Cryptocurrencies and future financial crime. *Crime Science*, 11:1-35.

Uniamikogbo, E., Adeusi, A.S. & Amu, U.C. 2019. Forensic audit and fraud detection and prevention in the Nigerian banking sector. *Accounting and Taxation Review*, 3(3):121-139.

Ünvan, Y.A. 2020. Financial crime: A review of literature. *Contemporary Issues in Audit Management and Forensic Accounting*, 102:265-272.

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

Van Niekerk, M.G. & Phaladi, N.H. 2020. Digital financial services: Prospects and challenges. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, *23*(1).

Vanani, I.R. & Shaabani, A., 2021. Digital transformation: Utilization of analytics and machine learning in smart manufacturing. In *Artificial Intelligence, Machine Learning, and Data Science Technologies* (pp. 269-281). CRC Press, Boca Raton.

Verma, A., Taneja, A., & Arora, A. 2017. Fraud detection and frequent pattern matching in insurance claims using data mining techniques. In 2017 *Tenth International Conference on Contemporary Computing (IC3)*. Noida, India,10-12 August. IEEE.

Voitsekh, V.O., 2022. Retrospective Analysis of the Word "Digitalization". *Business, Economics, Sustainability, Leadership and Innovation*, (9):4-9.

Vozniuk, A.A., Savchenko, A.V., Tarasevych, T.Y., Dudorov, O.O. & Klymenko, O.A. 2020. Electronic money and payments as means of committing crimes. *Academic Journal of Interdisciplinary Studies*, *9*(4):150-159.

Walliman, N. 2017. Research theory. In *Research methods: the basics* (pp. 16-30). Routledge, London.

Walsham, G. 1997. Actor-network theory and IS research: Current status and future prospects. *Information Systems and Qualitative Research*, 466-480.

Walsham, G. 2006. Doing interpretive research. *European Journal of Information Systems*, 15(3):320-330.

Wang, Y. & Hajli, N. 2017. Exploring the path to big data analytics success in healthcare. *Journal of Business Research*, 70:287-299.

Wanzer, D.L., 2021. What is evaluation?: Perspectives of how evaluation differs (or not) from research. *American Journal of Evaluation*, 42(1):28-46.

Weller, J., Migenda, N., Liu, R., Wegel, A., von Enzberg, S., Kohlhase, M., Schenck, W. and Dumitrescu, R., 2023, March. Towards a systematic approach for Prescriptive Analytics use cases in smart factories. In *International Conference on Machine Learning For Cyber-Physical Systems* (pp. 89-100). Cham: Springer Nature Switzerland.Wells, G., 2002. The role of dialogue in activity theory. *Mind, culture, and activity*, 9(1):43-66.

West, J. & Bhattacharya, M. 2016. Intelligent financial fraud detection: A comprehensive review. *Computers & security*, 57:47-66.

White, T. 2018. Reported economic crime in South Africa hits record levels. Available: https://www.pwc.co.za/en/press-room/. Date Accessed 30 June 2022.

Yamen, A., Al Qudah, A., Badawi, A., & Bani-Mustafa, A. 2019. The impact of national culture on financial crime. *Journal of Money Laundering Control*, 22(2):373-387.

Yaqot, M. and Menezes, B.C., 2021, August. Unmanned aerial vehicle (UAV) in precision agriculture: business information technology towards farming as a service. In *2021 1st international conference on emerging smart technologies and applications (eSmarTA)* (pp. 1-7). IEEE.

Yeboah-Boateng, E.O. and Kwabena-Adade, G.D., 2020. Remote access communications security: Analysis of user authentication roles in organizations. *Journal of Information Security*, 11(03):161.

Yeoh, P. 2019. Artificial intelligence: accelerator or panacea for financial crime? *Journal of Financial Crime*, 26(2):634-646.

Yin, R. K. 2015. *Qualitative research from start to finish*. Guilford publications, 2th edition, New York, USA.

Yong, B.X. 2019. Deploying machine learning under uncertainty for cyber-physical manufacturing systems, Master's thesis, University of Cambridge.

Young, J.C., Rose, D.C., Mumby, H.S., Benitez-Capistros, F., Derrick, C.J., Finch, T., Garcia, C., Home, C., Marwaha, E., Morgans, C. and Parkinson, S., 2018. A methodological guide to using and reporting on interviews in conservation science research. *Methods in Ecology and Evolution*, 9(1):10-19.

Yulianto, H., 2021. Philosophy of Management Science: Ontology, Epistemology, and Axiology Perspectives. *Cross-Border Journal of Business Management*, 1(1):152-162.

Zweni, A. & Yan, B. 2022. The role of municipal officials in financial crimes and the effects thereof: A conceptual framework to combat financial crimes in South African Municipalities. *African Renaissance*, 19(3):35-57.

APPENDICES

APPENDIX A: INTERVIEW GUIDELINE

1. Financial crimes happen in many organisations. Do you agree?
        a. If yes, why do you agree?
    2. What are some of the types of financial crimes that have happened in the few months or years, in the organization?

3. In your view, why do you think some of these crimes happened?

4. How do you think these financial crimes currently being prevented or mitigated?

5. Why do you think such approaches are adopted?
6. Does the organization use any data analytics to monitor or track these financial crimes?
        a. If yes, why? If no, why?
        b. In your view, how was the tool selected?

7. In your view, what are some of the challenges in tracking these financial crimes?

8. Why do you think these challenges exist?

9. Have the organization explored detective analytics?
        a. If no, why not? If yes, why?
10. What do you think is the organisation’s experience with detective analytics?
11. In your view, do you think detective analytics can help mitigate financial crimes?

12. why do you think so?
13. Do you think detective analytics awareness was raised in the Bank and people know how it can assist them?

APPENDIX B: INDIVIDUALCONSENT LETTER

Cape Peninsula
University of Technology

FID/REC/ICv0.1

FACULTY OF INFORMATICS AND DESIGN

Individual Consent for Research Participation

Title of the study: The instrumentation of Detective analytics for mitigating financial crimes in South African institutions

Name of researcher: Nontobeko Mlambo
Contact details: email: mlambononto@gmail.com phone: 0737693608

Name of supervisor: Tiko Iyamu
Contact details: email: Iyamut@cput.ac.za phone: 0716770300

Purpose of the Study: The research aims to develop an instrumentation, a tool that can be used to implement detective analytics to mitigate financial crimes.

Participation: My participation will consist essentially of (i) employee in the finance or IT department or division of the organisation; (ii) must have experienced crime in the organisation; (iii) must be knowledge about detective analytics; and (iv) part of the unit or department that provides, supports or manages mitigation solution.

Confidentiality: I have received assurance from the researcher that the information I will share will remain strictly confidential unless noted below. I understand that the contents will be used only for Doctor of philosophy in informatics and that my confidentiality will be protected by use of pseudonyms.

Anonymity will be protected in the following manner (unless noted below) will not mention any
identification of the participants *(Describe how anonymity will be guaranteed, e.g. if photos are being used, the blanking out of faces and/or places names. If anonymity cannot be protected, state this expressly, explain the reason why and explain the risks involved for the participant, the organization, etc).*

Conservation of data: The data collected will be kept in a secure manner CPUT: Data Management Plan *(Describe how and where the data will be stored, who will have access to it, and how long it will be conserved, e.g. digitally recorded interviews will be encrypted and kept in a password controlled environment. Note: original data or a copy of the data should be kept for audit purposes).*

Voluntary Participation: I am under no obligation to participate and if I choose to participate, I can withdraw from the study at any time and/or refuse to answer any questions, without suffering any negative consequences. If I choose to withdraw, all data gathered until the time of withdrawal will destroyed. I will use seek permission Change from participant to use collected data.

Additional consent: I make the following stipulations (please tick as appropriate):

	In thesis	**In research publications**	**Both**	**Neither**
My image may be used:				X
My name may be used:				X
My exact words may be used:	X			
Any other (stipulate):				X

Acceptance: I, (print name) *Mmapula Mmaga*____

agree to participate in the above research study conducted by Nontobeko Mlambo *(name of researcher)* of the Faculty of Informatics and Design: Information technology*(name of Department)* at the Cape Peninsula University of Technology, which research is under the supervision of Tiko Iyamu *(name of supervisor).*

If I have any questions about the study, I may contact the researcher or the supervisor. If I have any questions regarding the ethical conduct of this study, I may contact the secretary of the Faculty Research Ethics Committee at 021 469 1012, or email naidoove@cput.ac.za.

Participant's signature   Date: __24/04/2024________

Researcher's signature: _____________________   Date: 24/04/24

APPENDIX C: ETHICAL CLEARANCE

Cape Peninsula
University of Technology
creating futures

PO Box 1906, Bellville,7535 Symphony Way, Bellville, Cape Town, South Africa
+ 27 (0)21 959 6767 www.facebook.com/cput.ac.za info@cput.ac.za www.cput.ac.za

Office of the Research Ethics Committee
Faculty of Informatics and Design
Room 2.09
80 Roeland Street
Cape Town
Tel: 021-469 1012
Email: ndedem@cput.ac.za
Secretary: Mziyanda Ndede

9 May 2024

Miss Nontobeko Mlambo
c/o Department of Information Technology
CPUT

Reference no: 219040400/2024/6

Project title: The instrumentation of Detective analytics for mitigating financial crimes in South African institutions

Approval period: 9 Mayl 2024 – 31 December 2025

This is to certify that the Faculty of Informatics and Design Research Ethics Committee of the Cape Peninsula University of Technology approved the methodology and ethics of Miss Nontobeko Mlambo (219040400) for Doctor of Philosophy in Informatics.

Any amendments, extension or other modifications to the protocol must be submitted to the Research Ethics Committee for approval.

The Committee must be informed of any serious adverse event and/or termination of the study.

Prof L.J. Theo
Chair: Research Ethics Committee
Faculty of Informatics and Design
Cape Peninsula University of Technology