




The impact of legal framework on cyberfraud perpetration in the South African banking industry

 **Oluwatoyin Esther Akinbowale**¹⁺

 **Mulatu Fekadu Zerihun**²

 **Polly Mashigo**³

^{1,2,3}Faculty of Economics and Finance, Tshwane University of Technology, South Africa.

¹Email: oluwate01@gmail.com

²Email: zerihunmf@tut.ac.za

³Email: mashigomp@tut.ac.za



(+ Corresponding author)

ABSTRACT

Article History

Received: 2 September 2024

Revised: 6 December 2024

Accepted: 30 December 2024

Published: 14 January 2025

Keywords

Banking institution
Cyberfraud mitigation
Cyberfraud perpetration
Cyber-Laws
Legal framework
Regulatory policies.

This study examines the impact of legal framework on cyberfraud perpetration in the South African banking industry. The banking institution in South Africa is faced with the increasing rate of cyberfraud perpetration, which affects the performance of the banks, customer satisfaction, profitability, as well as banking reputation. This study combines the explanatory research approach, systematic literature review, and quantitative survey to investigate the impact of legal framework on cyberfraud perpetration in the South African banking industry. Initially, a total of 1579 literature were gathered from institution's report and academic database using search engines. However, the application of the inclusion criteria screened the literature to 50. Furthermore, a quantitative survey involving the use of a structured questionnaire and expert sampling of key organisational staff saddled with the responsibility of cyberfraud mitigation was conducted across the 17 licensed banks in South Africa, and the outcome was analysed in the Statistical Package for Social Sciences (SPSS) 2022 environment. The outcome of the review indicated the presence of legal frameworks, yet with an increasing rate of cyberfraud perpetration. Both the outcome of the review and survey criticised the non-stringent nature of the cyber laws and the non-implementation of some of its provisions.

Contribution/Originality: The novelty of this study lies in the combination of the explanatory research approach and systematic literature review for investigating the impact of legal framework vis-à-vis cyberfraud mitigation. The study contributes to the understanding of the legal framework that can assist policymakers in their quest for effective cyberfraud mitigation.

1. INTRODUCTION

In South Africa, as contained in the Electronic Communication and Transaction Act (ECTA) of 2002, cyberfraud refers to any criminal activity carried out via the use of electronic communications or information systems or any device connected to the internet (Government Gazette Republic of South Africa, 2002). The banking institution in South Africa is faced with the increasing rate of cyberfraud perpetration, which affects the performance of the banks, customer satisfaction, profitability, as well as banking reputation. South Africa tops the list of African countries with the highest number of cybersecurity threats, with a total of 230 million threats detected between 2020-2021, which reportedly cost the country the loss of R2.2 billion a year (INTERPOL Report, 2022). The increase in the rate of cyberattacks in South Africa is connected to the evolution of digital banking, such as online or mobile banking (Akinbowale, Klingelhöfer, & Zerihun, 2020; INTERPOL, 2021). INTERPOL Report

(2022) also reported that there were cases of business email compromise (BEC) and ransomware threats in South Africa between 2020-2021. Globally, South Africa holds the fifth position in the cybercrime density ranking, with an 8% increase in cybercrime victims among specific internet users from 2021 to 2022 (Surfshark, 2022). Although the banking institution has regulatory policies that are implemented, the rate of cyberfraud perpetration is still high. The country recognises the need for more stringent cybersecurity systems; inadequate resources in terms of financial and human resources continue to impede the efforts. Cassim (2011) established a connection between the rise in cybercrime in Africa, relative to other continents, and the increasing number of Internet users. The report of the International Finance Corporation (2020) indicates that the African internet economy represents a large investment opportunity, which has great potential to drive the Africa's economy and development. With the growing rate of Africa's population and the internet users, the internet economy has the potential to increase Africa's gross domestic product (GDP) by \$180 bn by 2025. This accounts for 5.2% of the total continent's GDP, and by 2050, it is projected that the internet economy could potentially contribute US\$712bn to the continent's GDP, accounting for 8.5% of the total continent's GDP.

The International Finance Corporation (2020) further indicates that the internet economy is gradually transforming the efficiency and productivity of critical industry; hence, the internet economy plays a fundamental role in Africa's drive towards e-commerce, increasing GDP growth as well as the increasing rate of foreign investors' interest. However, the internet also presents a potential risk for individuals, investors, businesses, and governments who are vulnerable to cyberfraud perpetration.

INTERPOL Report (2022) reported that the rate of internet penetration in South Africa has increased to over 70%. Thus, cyberfraudsters may exploit the vulnerabilities of cyberspace to perpetrate fraud.

Another area with an increasing rate of fraud perpetration in South Africa is the cryptocurrency fraud. INTERPOL reported that South Africans were scammed out of \$588 million and \$3.6 billion in Bitcoin in 2020 and 2021, respectively. Cryptocurrency fraud is escalating in South Africa, with the country named among the top ten countries with the highest rate of cryptocurrency fraud globally. Furthermore, threat actors also engage in phishing and other forms of social engineering to acquire sensitive information from unsuspecting victims to steal funds from their accounts.

Existing studies such as Sutherland (2017); Du Toit, Hadebe, and Mphatheni (2018) and Dlamini and Mbambo (2019) identified the weak cybercrime legislative framework of South Africa as one of the reasons for the increasing rate of cyberfraud perpetration. The threat actors often take undue advantage of the weak cyber laws, as well as inadequate capacities (such as technical support and training of the law enforcement agencies) to perpetrate cyberfraud. Although the South Africa's Cyber Crime Bill was adopted as a law in 2021 to strengthen the legal framework and promote cybercrime mitigation, the law is still yet to be fully implemented. Allen (2021) stated that the non-implementation of some of the sections of the cybercrime legislation is an indication of deficient expertise and resources. Hence, in recent times, the country still suffers from major cybercrime attacks, coupled with the fact that the country is still listed among countries with the highest rate of cybercrime perpetration in Africa and world at large. Surfshark (2022) indicated that the country tops the list of African countries with the highest rate of cybercrime perpetration and placed fifth globally in terms of cybercrime density (percentages of victims of cybercrime among specific internet users). Thus, the motivation for this study arises from the need to promote cyberfraud mitigation in South Africa through effective legislation. South Africa may achieve sustainable and effective cybercrime mitigation through legal reforms, including the development and implementation of more stringent cyber laws.

Thus, this study aims to investigate the impact of legal framework on cyberfraud perpetration in the South African banking industry using the combined approach of explanatory research and systematic literature review.

To achieve this aim, three research questions were framed as follows:

1. What are the root causes of cyberfraud perpetration in the South African banking industry?

2. What is the impact cyberfraud perpetration on the South African banking industry?
3. What is the impact of legal framework on the rate of cyberfraud perpetration in the South African banking industry?

The research questions were answered via explanatory research comprising in-depth literature review, and survey. The first two were answered by drawing inferences from literature review while the last research question was answered from the outcome of the quantitative survey.

This study is significant in that it adds to the understanding of the legal framework that will assist policy and decision-makers to improve on the current legal framework for effective mitigation of cyberfraud in South Africa. Secondly, the survey conducted helps to understand the perception of experts in the South African financial institution about the efficacy, stringency, implementation and impact of the cyber laws. The outcome of this study may assist the legislators, government, security agencies, policy and decision-makers in achieving legal reforms geared towards cyberfraud mitigation. This may include the review of the existing laws and the enactment of a more combative law in the future or the review of existing regulatory policies to adequately address the dynamic and emerging trend of cyberfraud perpetration. This outcome of this study may also promote the implementation of the cyber law, which is crucial to cybercrime mitigation. A necessary step towards data protection and reduction in cybercrime perpetration in South Africa is the integration of the Cybercrimes Act into the legislative framework.

The structure of this study is as follows: the first section presents the introduction, which comprises the background to the study, motivation, statement of the problem, aim, research questions, and significance of the study. The subsequent section highlights the methodology used in this study, majorly the combination of the explanatory research approach and systematic literature review. Section 3 presents the details of the systematic literature review conducted, while section 4 details the results and discussion. The last section presents the conclusion and recommendations as well as directions for future studies.

2. METHODOLOGY

This study combines the explanatory research approach and systematic literature review on the impact of legal framework on cyberfraud perpetration in the South African banking industry.

2.1. Explanatory Research Approach

The explanatory research is an approach that can be used to investigate the occurrence of a phenomenon. This type of research can be employed to gain a detailed understanding about the root cause of a phenomenon (Bentouhami, Casas, & Weyler, 2021). Thus, it was employed in this study to investigate the root cause of cyberfraud perpetration in the South African banking industry. The explanatory research approach was conducted in six steps (Figure 1) itemised as follows:

- Step 1: Definition of the problem.
- Step 2: Formulation of research questions.
- Step 3: Development of methodology.
- Step 4: Gathering of data.
- Step 5: Analysis of findings.
- Step 6: Development of avenues for further research.



Figure 1. The explanatory research approach steps.

2.2. Systematic Literature Review

The systematic literature review was employed for the investigation of the impact of legal regulation on cyberfraud perpetration in the South African banking industry. The systematic literature review is suitable for the synthesis of existing studies and reports to gain a detailed understanding of the investigated phenomenon. The approach is also suitable for achieving a critical review and summary of existing literature with reduction in bias so as to draw a valid conclusion (Daniyan, Mpofu, Ramatsetse, & Gupta, 2021; Maware, Muvunzi, Machingura, & Daniyan, 2024). This study investigates the impact of legal framework on cyberfraud perpetration in the South African banking industry. This was achieved via the use of an explanatory approach and systematic literature review. The systematic literature conducted according to the guiding principles of the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) as stated by Page et al. (2021). First, the aim, scope, and research questions were defined. This was followed by the identification of data sources. The study conducts desktop research using data sourced from both grey and empirical literature. Search engines such as Google were employed for searching the literature online using keywords that relate to the subject matter, such as “South African banking industry,” “cyberfraud,” “cybercrime,” “cyber laws,” “cybersecurity,” “legal framework,” “regulatory framework,” “cyberthreats,” “cyberfraud perpetration,” etc., were searched through academic databases such as ResearchGate, Google Scholar, digital library, BASE, Science Direct, Directory of Open Access Journals, Scopus, IEEE, and Web of Science, etc. The search process was conducted with the use of single keywords such as “banking,” “regulations,” etc., and combinations of words such as “financial regulations,” “legal framework,” etc. The Boolean operator ‘AND’ was employed for the combination of the keywords such as “banking crises and resilience,” and “banking and risk management. Wildcards, * and? were also employed for the identification of the various forms of the keywords. Some of the limitations of the systematic literature review as it applies to this study include the risk of bias during the selection and synthesis of the articles as well as the screening of the initial articles gathered without excluding relevant ones. To mitigate these limitations, the inclusion and exclusion were clearly defined, and the selection and synthesis of the articles were taken through a rigorous process leading to a consensus method for resolving discrepancies. The inclusion criteria include the significance of the titles and abstracts to the subject investigated to identify potentially relevant studies (this was used for the initial screening of articles), types of studies (empirical, conceptual, and theoretical studies were considered), year of publication (78% of the articles must not be older than ten years), language (articles written only in English were considered), and the nature of review process undertaken before publication (peer review articles were mostly considered to ensure the validity of

the findings). Initially, 1579 articles were obtained from the various databases, out of which 321 identical articles were removed. Furthermore, 121 unidentified articles were eliminated, while 67 articles were excluded due to the fact that they were not presented in English. Other exclusion criteria include the relevance of the title as well as the year of publication, which led to the elimination of 218 articles. Furthermore, 507 articles were further eliminated due to their irrelevant titles, abstracts, focus, and lack of empirical findings, while 273 articles were excluded because they did not answer the research questions. Finally, a total of 50 peer-reviewed articles whose bearing aligns with the subject matter were reviewed. These articles contributed empirically, conceptually, and theoretically to the literature on cyberfraud, its rate of perpetration in the South African banking industry, and the impact of legal or regulatory frameworks on the rate of perpetration. To minimise errors and bias during the article screening and synthesis process, the three authors of this study brainstormed to screen and synthesise the selected articles using the exclusion and inclusion criteria. Figure 1 presents the PRISMA diagram, which details the selection of the articles reviewed. The relevant themes and outcomes of the study include “causes of cyberfraud perpetration in the South Africa’s banking industry” and “impact of the Cybercrimes Act” on the South Africa’s financial institutions. Figure 2 presents the PRISMA diagram.

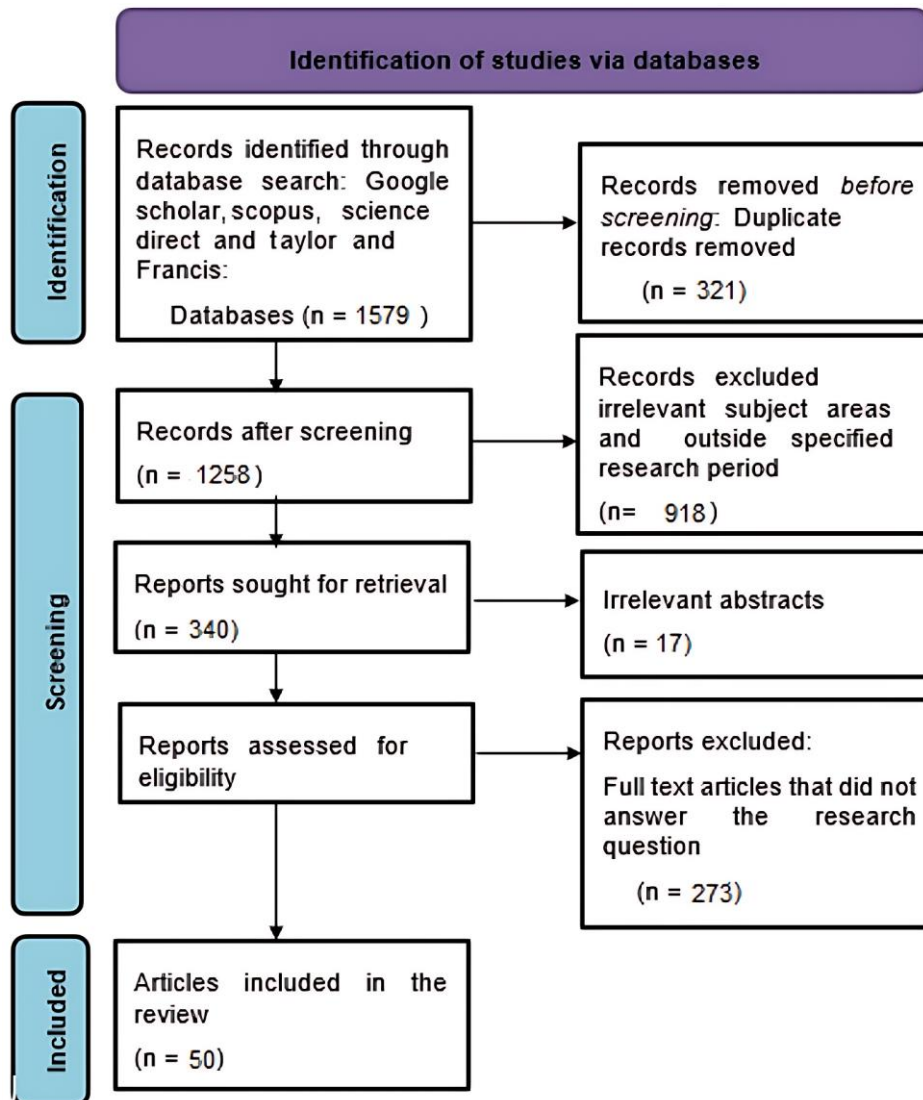


Figure 2. The PRISMA diagram.

2.3. Survey

This study employed the quantitative approach, comprising the use of structured questionnaires as the survey instrument. The quantitative analysis is useful for gathering quantifiable data and obtaining numerical statistics of a simple or complex phenomenon and is also suitable for hypothesis testing (Assessment Capacities Projects (ACAPS), 2012; Juran, 2019; Mohajan, 2018; Surendran, 2019).

Expert sampling was employed as the sampling method because it allows the participation of specific individuals who have experience and are knowledgeable about the phenomenon under investigation (Anon, 2020). Questionnaire is suitable for gathering and quantifying information on sensitive phenomena such as cyberfraud (Oppenheim, 1992; Wilson & McClean, 1994).

The expert sampling was carried out across key organisational staff in charge of cyberfraud mitigation across the 17 licensed banks in South Africa, and the outcome of the survey was analysed in the Statistical Package for Social Sciences (SPSS) 2022 environment. Data was gathered from the forty-two members of staff of the 17 South African licensed banks. Although the survey was carried out in Pretoria, Gauteng Province, the outcome was reflective of the current situation in the South African banking industry in terms of cyberfraud perpetration and mitigation. This is because the South African banks have the same mode of operation and are centrally regulated by the South African Reserve Bank (SARB). This implies that the sampled banks are representative of the country as a whole. The structured questionnaire has multiple choices that capture the quantitative data.

The questionnaire was made available to forty-two banks' staff, including top management, forensic experts, fraud examiners, customer relations officers, and computer analysts.

The use of questionnaires was informed by their suitability for capturing, quantifying, and verifying a complex challenge such as cyberfraud. Besides, it also enables the collection of information from respondents in a time-effective and standardised way (Oppenheim, 1992; Wilson & McClean, 1994).

The structured quantitative comprises of the ordinal data type (Likert-type response format) with clear and simplified questions and instructions to avoid the challenge of non-response bias. All the questions administered to the respondents received a confirmatory outcome, thus, eliminating the problem of non-response bias.

The responses gathered from the administered questionnaires were further sorted and analysed to avoid a biased point of view. Thereafter it was analysed in the SPSS environment, and the Chi-square as well as the Fischer Exact tests were conducted to test the hypothesis.

3. LITERATURE REVIEW

3.1. Theoretical Framework

This study incorporates the rational choice theory (RCT) by Cornish and Clarke (1987) and the routine activity theory (RAT) developed by Cohen and Felson (1979). The RCT opines that humans are reasoning actors who weigh the benefits and consequences of actions before making a rational choice. In the context of this study, when there is a strong consequence for cyberfraud perpetration as provided by the law, it may act as a deterrent for the threat actors. Similarly, RAT posited that for a crime to be perpetrated, there must be a vulnerable target, a likely and willing offender, and an absent guardian that is capable of preventing the perpetration (Holt & Bossler, 2008). The RCT insists that crime is an organised and deliberate behaviour aimed at maximising personal gains, while the RAT accounts for the likelihood of fraud perpetration via the exploitation of available opportunity. These theories provide useful insights for the formulation of policies and strategies for crime prevention; however, the criticism of the RCT is that offenders are rational in their thinking and decision-making (Leukfeldt & Yar, 2016) while the critics of RAT indicated the lack of consideration of social economic factors such as unemployment, gender inequalities, and poverty, which may contribute to the motivation for fraud perpetration (Clarke & Felson, 1993). Drawing from the two theories, it is clear that the presence of stringent legislation could make the consequences

outweigh the benefits, as in the case of the RCT, while the stringent cyber laws and the enforcement agencies, such as the police, can act as capable guardians against fraud perpetration.

3.2. Causes of Cyberfraud in the South Africa Banking Industry

Some of the probable causes include weak cybersecurity laws, installation and use of emerging technologies, weak controls by the management, poor organisation culture, inadequate documentation, lack of ethical culture, overrides of internal control by the management, and absence of accountability (Akinbowale, Klingelhöfer, Zerihun, & Mashigo, 2024). According to INTERPOL (2021) some possible reasons for South Africa's increase in cyberattack include cyber insecurity, low public awareness, poor enforcement of cyber law, and inadequate training for security personnel (INTERPOL, 2021).

Snail ka Mtuze and Musoni (2023) argue that South Africa is no longer a safe place for cybercriminals with the promulgation of cyber laws to complement the existing legal frameworks and the operationalisation of some sections of the existing laws. However, the authors noted the need for sensitization, training, and human capacity development for the security and legal stakeholders, such as the police, legal practitioners, magistrates, and judges, on cybercrime and cyber laws as well as electronic evidence gathering and its admissibility for effective prosecution of the culprits.

Snail ka Mtuze and Musoni (2023) suggested the engagement of skilled experts, such as forensic accountants, to assist in the process of evidence gathering and cybercrime investigations. The authors also suggested the need to improve on the services provided by the Specialised Commercial Crimes Courts in South Africa. CMS Law (2024) stated that the effectiveness of South Africa's new Cybercrimes Act in mitigating cybercrime depends on its enforcement and implementation by security agencies, technological advances, and adaptability, which necessitate periodic review and amendment of the law to tackle evolving trends of cybercrime, international cooperation, and public-private sector collaboration.

Cassim (2011) indicates the need for effective formulation and implementation of cybersecurity laws and underscores the importance of collaboration of security agencies at all levels to combat cyberfraud since it is a cross-border crime. Some of the efforts of INTERPOL (2024) aimed at fighting cyberfraud at the regional level include

- Provision of intelligence reports and activities coordination of operations to dismantle the networks of the threat actors.
- The security agencies are developing their regional capacity.
- Public sensitisation and awareness about the operations of the threat actors.

Internal controls can be implemented at the organisational, or transaction levels or as a combination of both. At the organisation's level, internal controls regulate the organisation's and employees' activities to ensure that the goals of the organisation are met (Shahbuddin, Alam, & Azad, 2011). At the transaction level, internal control are control procedures to monitor or minimise variations in financial processes to promote the integrity and security of business transactions. According to Shahbuddin et al. (2011) effective internal controls can promote the reliability of financial transactions, reporting, and regulatory compliance. However, the achievement of an organisation's goal as well as the reliability of financial transactions is not only a function of a robust internal control but also functions of other factors such as the implementation of technological solutions (Shahbuddin et al., 2011).

In terms of fraud mitigation, effective internal control can aid the processes of fraud detection and prevention. These include the detection of the scenarios that could lead to fraud and the response action to prevent the fraud or mitigate the risk as well as risk management policies. Hence, internal control can also ensure systematic improvement in business performance. Internal control can also enhance financial information flow, which is necessary for cyberfraud mitigation (Shahbuddin et al., 2011). Thus, a robust internal control measure may promote proactiveness in fraud mitigation; therefore, continuous commitment of an organisation's top management to

internal controls may help sustain the fight against cyberfraud. Mohd-Sanusi, Mohamed, Omar, and Mohd-Nassir (2015) stated that effective internal control can lessen the risk and reduce the likelihood of fraud. Other areas of application of internal controls as they relate to cyberfraud perpetration include the monitoring of the implementation of operational procedures, standards code of conduct, certifications of all financial statements, authentication of financial transactions, as well as periodic reviews of reviews of internal controls measures and transactions by the management.

Another important aspect of internal controls that is critical to cyberfraud mitigation is regular assessment and vulnerability of an organisation's processes, operations, and systems to determine inherent threats and taking remedial actions where necessary.

To reinforce the internal controls of the South African banking industry geared towards fraud prevention, Akinbowale, Klingelhöfer, and Zerihun (2023) conducted a survey in South African banks, and the outcome indicates a positive relationship between fraud risk management and forensic accounting implementation. Thus, the authors proposed the incorporation of forensic accounting techniques into the control framework of the South African banks for fraud risk mitigation.

3.3. Overview of the Legal Framework against Cybercrime in South Africa

South Africa has made some legal efforts geared towards reducing cybercrime. For instance, the Electronic Communication and Transaction Act (ECTA) of 2002 aimed at facilitating and regulating electronic communication and transaction to protect financial institutions and the public (Government Gazette Republic of South Africa, 2002). However, the criminal section of the ECT was critiqued as a weak measure (Cassim, 2011). It is widely perceived as non-stringent; thus, it might not adequately serve as a deterrent to the offenders. In 2013, the Protection of Personal Information (POPI) Act was enacted by the South African government as part of the measures to guarantee confidentiality of personal data, while in 2015, the National Cyber Security Policy Framework (NCPF) enforced by the Ministry of State Security was also passed to promote cybersecurity (Sutherland, 2017). Following the passage of the new Cybercrimes Act 19 of 2020 ("Act") into law in 2021, the law clearly defines cybercrime and identifies the offences that constitute cybercrimes. In the South African context, cybercrime includes any activity such as intrusion into individual or corporate computers or electronic devices (including USB drives or external hard drives), unlawful access, interruption, or acquisition of data; the illegal procurement, control, receipt, or use of an individual or organisation's confidential information (such as passwords), falsification, fraud, or online extortion, and suspicious communications (Allen, 2021). The law empowers the South African police service to conduct searches and seizures of exhibits suspected to be used for cybercrime perpetration. By the law, the South African police service is empowered to conduct domestic investigations with respect to cyberfraud perpetration, including evidence collection and preservation. Since cybercrime is a transborder crime, the legislation prescribes international cooperation and information sharing.

There is a correlation between the POPI Act and the Cybercrimes Act. The POPI Act deals with data privacy, while the Cybercrime Act deals with cybersecurity. Thus, by achieving data privacy and cybersecurity, the rate of cybercrime perpetration may reduce if the laws are fully implemented.

South Africa has been a target of cybercriminals as a result of lack of awareness of cybersecurity and lack of enforcement of cybersecurity law in the country. However, with the new Cybercrimes Act 19 of 2020 ("Act"), which has commenced partial implementation, the prosecution of the threat actors and fight against cybercrime may be more sustainable.

The new Cybercrimes Act 19 of 2020 ("Act") considers the various channels exploited by cybercriminals to commit crime, and the Act is now an integral part of the South Africa's legislative framework on data

protection. This gives the security, legal practitioners, and judiciary a basis for the investigation and prosecution of offenders.

The Act empowered the South African Police Service (SAPS) to conduct investigations, search, access, or seize any computer, or network, or database, on condition that they possess a search warrant (The South African Government, 2021). Thus, the Minister of Police is saddled with the responsibility to establish a point of contact for cybercrimes and detect, prevent, and investigate cybercrimes. As such, victims (individuals or institutions) of cybercrime can provide reports to the SAPS or seek assistance from the point of contact (The South African Government, 2021). This agrees with the position of McEwan, Mullen, and MacKenzie (2010) that there is a need for a thorough search during the investigation and detection processes of cyber-related crime. This includes a thorough search of suspected systems or computer terminals, as well as the servers and all related computer hardware and software.

Some of the impacts of the Cybercrimes Act on the South Africa's financial institutions include:

3.3.1. Reporting Obligation

Section 54 of the Cybercrimes Act imposes reporting obligations on the South Africa's financial institutions. This section mandates financial institutions, including their service providers, to report cybercrime incidence to the South African Police Service within 72 hours of noticing the threat or crime. According to the Act, regulatory bodies such as SARB and the Financial Sector Conduct Authority (FSCA) are excluded from the chain of reporting obligations according to the section 54 of the Cybercrimes Act (The South African Government, 2021).

However, some of the drawbacks of this section of the Act is that it has not taken full effect yet, and the Act does not impose the task of monitoring the data either transmitted or stored on the financial institutions or service providers. Furthermore, the Act does not mandate the financial institutions or service providers to critically investigate the circumstances that led to the preparation of the illicit activity.

3.3.2. Obligation of Offering of Assistance During Investigations

Financial institutions are mandated by the act to furnish the SAPS with the needed technical or other assistance required to search, access, or seize any data or computer that may be linked to a cybercrime (The South African Government, 2021). However, the Act did not state precisely the nature of assistance to be provided by the financial institution.

3.3.3. Data Storage Obligations

Financial institutions are expected to retain any information that may be useful for the South African Police Service during cybercrime investigations (The South African Government, 2021). Once the financial institutions or service providers detect an illegal activity of a threat actor via the institution's system or network, a cybercrime, the institution is mandated to retain the associated the data for an unspecified period to assist the police service during investigations. However, the Act did not state precisely the time frame for the retention of the data by the financial institutions or service providers or the timeline for the commencement of the investigation by the police once reported by the financial institutions or service providers.

Allen (2021) criticises the non-implementation of some of the provisions of the new Cybercrimes Act while identifying shortage of expertise in the ranks of the South African Police Service as a major hindrance to the full implementation of the Act.

3.3.4. Data Processing Obligation

The Cybercrimes Act mandates organisations to review their data processing techniques and practices and adhere to practices that will prevent the perpetration of cyber-related crimes defined in the Cybercrimes Act.

Louw (2012) argued that effective formulation and implementation of cybercrime prevention laws and programmes require the knowledge of the prevalent forms of cyber-related crimes, the probable causes, the physical and social features of the environment, the roles of various institutions in tackling the crime, among other things. Graham and Bennett (2013) indicated the need for public sensitisation in community-based crime with an emphasis on the consequences of being caught to reduce the attempt of perpetration by potential offenders. Furthermore, Graham and Bennett (2013) indicated that the prosecution of cyber-related crime is challenging because of the cross-border nature of the crime and the issue of inter-jurisdiction.

Hence, international cooperation as well as engagement of skilled investigators and prosecutors, such as forensic experts, will be required (Mandia, 2011).

4. RESULTS AND DISCUSSION

4.1. Unveiling the Root Causes of Cyberfraud Perpetration in the South African Banking Industry

Table 1 presents the root causes of cyberfraud perpetration in the South African banking industry obtained from the synthesis of the literature, while Figure 3 presents the data points of the supporting literature.

Table 1. The root causes of cyberfraud perpetration extracted from the literature review.

S/n	Causes	References
1.	Innovations, technological advances, or developments such as digitalisation of financial operations	Dagada (2013); Sutherland (2017); Dzomira (2015); Dzomira (2017); Coetzee (2018); Dlamini and Mbambo (2019); Barlow (2023) and Akinbowale et al. (2024)
2.	Weak or lack of stringent cybersecurity laws and non-implementation of the enacted laws	Cassim (2011); Sutherland (2017); Du Toit et al. (2018); Dlamini and Mbambo (2019); Allen (2021); Chitimira and Ncube (2021) and Akinbowale et al. (2024)
3.	Weak controls by the management: poor organisational culture, inadequate documentation, lack of ethical culture, overrides of internal control by the management, and absence of accountability	Dlamini and Modise (2012) and Akinbowale, et al. (2023)
4.	Socioeconomic factors such as high rates of poverty, inequality, high rates of employment, and inadequate skilled labour to combat cyberattack	Dzomira (2017); Barlow (2023) and Akinbowale et al. (2024)
5.	Lack of up-to-date cybersecurity systems, weak cyberdefense	Grobler and Louwrens (2009); Dlamini and Modise (2012); Mbelli and Dwolatzky (2016); Dzomira (2017); Chitimira and Ncube (2021); Barlow (2023) and Akinbowale et al. (2024)
6.	Low awareness and inadequate public sensitisation	Cassim (2011); Dlamini and Modise (2012); Dzomira (2017); Du Toit et al. (2018); Kshetri (2015) and Kshetri (2019)
7.	Weak fraud risk management framework	Cassim (2011) and Dlamini and Mbambo (2019)
8.	Weak regulatory/Policy framework	Akinbowale et al. (2024)

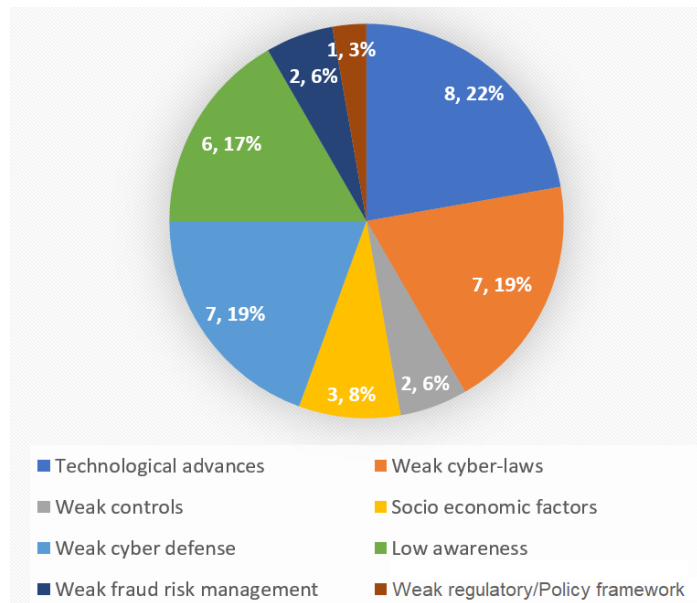


Figure 3. The data points on the root causes of cyberfraud perpetration from the literature.

4.2. Unveiling the Impact of Cyberfraud Perpetration in the South African Banking Industry

The outcome of the literature review indicated that the South African banking institution is faced with the increasing rate of cyberfraud perpetration with negative effects on the performance of the banks, customer satisfaction, profitability, as well as banking reputation (Akinbowale, et al., 2023; Akinbowale et al., 2024). The Information Security Institute (2013) outlined some of the impacts of cyberfraud perpetration as: information loss, loss incurred in the form of compensation to victims, business, service, and cyberinfrastructure disruptions, cost implications in terms of investigation, and development of countermeasures, loss of competitiveness due to loss of goodwill, as well as revenue or financial loss, which may affect the business’s profitability.

4.3. Results Obtained from the Survey on the Impact of Legal Framework on the Rate of Cyberfraud Perpetration in the South Africa Banking Industry

Table 2 presents the inquiry into the South African legal framework in relation to cyberfraud mitigation and the results obtained. This is depicted by Figure 4. The opinions of majority of the respondents are that the impact of legislations on cyberfraud mitigation is high, although some of the provisions of the cybercrime laws are not implemented. The respondents also acknowledged that the current cybercrime laws lack sufficient rigor and that they need review or amendment.

Table 2. Outcome of the inquiry into the legal framework.

Inquiry into the legal framework	Responses					Total percent response (%)
	Agree	Strongly agree	Disagree	Strongly disagree	Undecided	
The impact of legislations on cyberfraud mitigation is high (Q1)	16 (38.09%)	2 (4.76%)	14 (33.33%)	8 (19.05%)	2 (4.76%)	100
Some of the provisions of the cybercrime laws are not implemented (Q2)	17 (40.47%)	16 (38.09%)	6 (14.28%)	2 (4.76%)	1 (2.38%)	100
The cybercrime laws are not stringent enough (Q3)	22 (52.38%)	8 (19.05%)	6 (14.28%)	5 (11.90%)	1 (2.38%)	100
There is a need for review or amendment of cybercrime laws due to high rate of cyberfraud perpetration (Q4)	21 (50.00%)	15 (35.71%)	4 (9.52%)	1 (2.38%)	1 (2.38%)	100

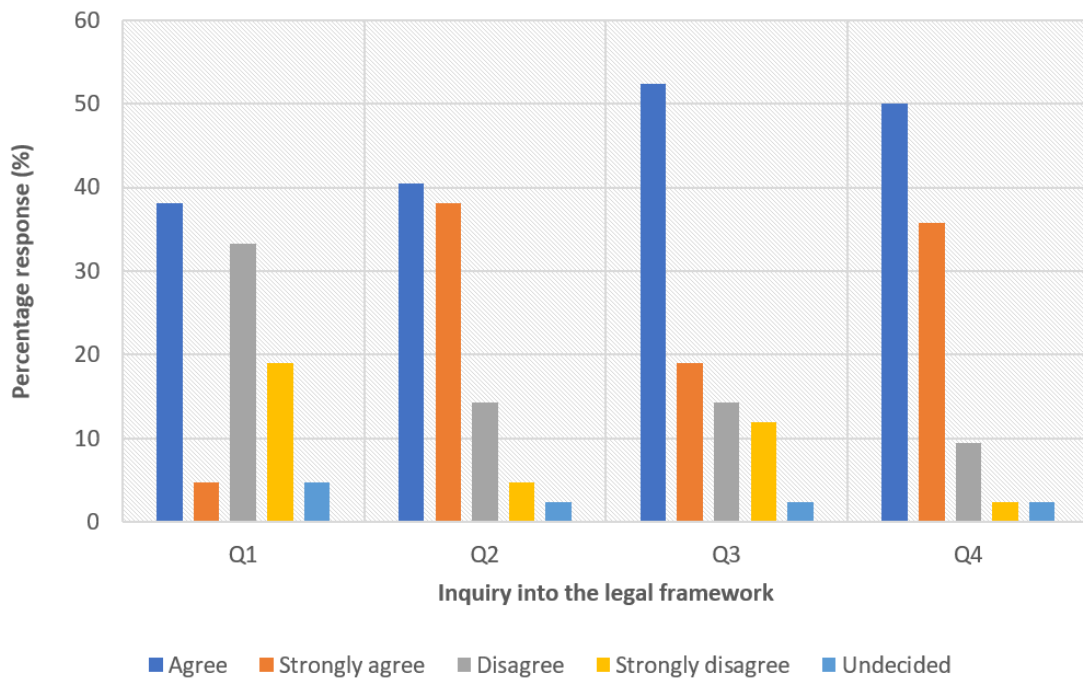


Figure 4. The implications of the legal framework vis-à-vis cyberfraud mitigation.

Table 3 displays the outcome of the Chi-square and Fischer’s Exact tests for the implications of the legal framework vis-à-vis cyberfraud mitigation. According to the results, there is insufficient evidence to accept the null hypothesis at a 5% level of significance. The justification for this conclusion is based on the fact that the *p*-values of the variables are less than 0.05. Thus, the alternative hypothesis is presumed to be true. This indicates the non-stringency of the cyberlaws and the non-implementation of some of its provisions, which calls for the investigation into the level of compliance as well as a review of existing cyber laws and regulatory policies.

Table 3. The outcome of the Chi-square and Fischer’s exact tests for the implications of the legal framework vis-à-vis cyberfraud mitigation.

Variables	Chi-square statistics	df	Asymptotic significance	Fischer’s exact sig.	Point probability
Q1	20.381	4	0.000	0.000	0.000
Q2	27.762	4	0.000	0.000	0.000
Q3	20.286	3	0.000	0.000	0.000
Q4	13.000	2	0.002	0.002	0.000

4.4. Discussion of Results

In order to promote cybersecurity, the services of the South African police alone as the law enforcement agency and investigator may be insufficient. Thus, a collaborative effort of the national cyber defence and security stakeholders involving the government, public and private sectors, national security agencies, and public will be helpful (Dlamini & Mbambo, 2019; Grobler, Van Vuuren, & Zaيمان, 2013). Gottschalk (2010) stated that law enforcement processes require mobilisation of resources, information sharing, and collaborations with the law enforcement agencies at all levels. Gumbi (2017) also noted that cybercrime is multi-jurisdictional in nature. Hence, effective collaborations will be beneficial to sustaining the fight against cybercrime.

The Cybercrime Act does not impose the task of monitoring the data either transmitted or stored on the financial institutions or service providers. However, the crime is driven by data, and the role of data monitoring in the fight against cyberfraud cannot be overemphasised, being an integral part of preventive measures that can forestall cybercrime occurrence. The availability of quality data can assist fraud investigators in uncovering fraud (Mittal, Kaur, & Gupta, 2021). Frequent monitoring of data can create loopholes for fraud perpetration. Regular monitoring of data ensures that acquired data is checked for source, accuracy, anomalies, trends, or patterns and

quality. The process of cyberfraud investigation and prevention is data-driven, thus, lack of data, monitoring system may affect the risk mitigation and decision-making process, as well as the outcome of the investigation, and may also jeopardise the efforts geared towards cyberfraud prevention.

Shahbuddin et al. (2011) stated that an organisation's internal control with regular auditing and monitoring can enhance reliable financial reporting and financial information flow. Mohammed and Knapkova (2016) as well as Hasham, Joshi, and Mikkelsen (2019) also stated that the cyberfraud risk management involves customers' identification and authentication, transactions monitoring and detection of anomalies, as well as response to risk and cyberattacks. Hopkin (2010) stated that the process of fraud control necessitates the use of monitoring technologies, regular reviews and audits, or whistleblowing to obtain latent signs of fraud and report before it culminates into a fraud case. Some existing studies support the involvement of financial institutions and service providers in data monitoring for effective cyberfraud mitigation (Joel & Vyas-Doorgapersad, 2019; Oguda, Albert, & Byaruhanga, 2015).

Although the financial institutions or service providers are not mandated to critically investigate the circumstances that led to the perpetration of the illicit activity, it may be more productive if they are allowed to outsource experts such as external auditors, independent financial investigators such as forensic accountants, etc. Sometimes, the loopholes may be a negligence on the part of the financial institution hence the need for critical investigations.

Rather than relying solely on the police for cybercrime investigations, financial institutions or service providers with inadequate expertise to fight cyberfraud-related risks may consider the option of outsourcing it; otherwise, such organisations may be susceptible to cyber attack. McIntyre, Van Graan, Van Romburgh, and Van Zyl (2014) stated that South Africa needs the services of fraud investigators such as forensic accountants to combat fraud. Existing studies also support the outsourcing of forensic accountants by financial institutions for fraud detection, investigation, analysis, and litigation support (Akinbowale, et al., 2023; Akinbowale, Mashigo, & Zerihun, 2023; Enofe & Danjuma, 2015; Lakshmi & Menon, 2016; Mehta & Bhavani, 2017; Modugu & Anyaduba, 2013; Mushtaque, Ahsan, & Umer, 2015; Shimoli, 2015).

The Cybercrime Act required financial institutions to provide support during investigations. However, the Act did not state precisely the nature of assistance to be provided by the financial institution. The preciseness of the nature of assistance required from the financial institutions will remove ambiguity or complexity while offering the assistance based on the requirements. Time is also an important factor during cybercrime investigation, as the number of victims, scope, and cost of perpetration may increase with time. The Cybercrime Act specifies an ultimatum of 72 hours for financial institutions to report cyberfraud incidence but did not specify the time frame for the police to commence investigation.

Overall, the Cybercrime Act is a right step, although it may appear non-stringent in nature, coupled with the non-implementation of some of its provisions. However, Ajayi (2016) acknowledged some challenges that may hinder the enforcement of cybercrimes laws and policy. These include a lack of universal agreement on the nature of crime or activity that forms cybercrime; restrictions on legal powers for fraud investigation, prosecution, and access to computers; the lack of uniformity among the various laws that relate to cybercrime investigation, lack of capacity for extradition of offenders, and an absence of mutual legal assistance and international cooperation in cybercrime investigations, among others.

4.5. Summary of Findings

This study focuses on the investigation of the impact of legal framework on cyberfraud perpetration in the South African banking industry. The research questions were answered using a combination of the explanatory research approach, systematic literature review, and quantitative survey. The outcome of this study indicates that there are existing cyber laws in South Africa, yet the rate of cyberfraud perpetration remains high. This may be due

to non-implementation or non-stringency of some provisions of the cyber laws to deter the threat actors. This finding agrees significantly with the outcome of some existing literature that linked the rate of cyberfraud perpetration in South Africa to a lack of stringent legislation and poor implementation of anti-cybercrime laws as well as inadequately equipped law enforcement (Akinbowale, et al., 2023; Barlow, 2023; Dlamini & Mbambo, 2019; Dlamini & Modise, 2012; Grobler et al., 2013; Sutherland, 2017). Although Snail ka Mtuze and Musoni (2023) hold a contrary view that South Africa is no longer a safe place for cybercriminals with the promulgation of cyber laws to complement the existing legal frameworks and the operationalisation of some sections of the existing laws.

The implementation of the cyber law is a vital step to South Africa's goal of cybercrime mitigation. The integration of the Cybercrimes Act into the South Africa's legislative framework is an essential step geared towards data protection and reduction in the rate of cybercrime perpetration in South Africa.

5. CONCLUSIONS AND POLICY RECOMMENDATIONS

The outcome of the survey conducted opinions of majority of the respondents that the impact of legislations on cyberfraud mitigation is high, although some of the provisions of the cybercrime laws are not implemented. The respondents also acknowledged the inadequacy of the cybercrime laws, stating that they require review or amendment. While the Cybercrimes Act has been signed into law, some provisions, such as the reporting obligation by institutions, are yet to be implemented in an enforceable manner. However, financial institutions and service providers must develop an internal framework to ensure that the requirements of the Cybercrimes Act are adhered to. The internal framework should also emphasise human capacity development and training programmes to educate the staff to aid their understanding about these requirements and the penalties of non-compliance.

Some of the perceived limitations of the Act are that it does not impose the task of monitoring the data either transmitted or stored on the financial institutions or service providers. Furthermore, the financial institutions or service providers are not mandated to critically investigate the circumstances that led to the perpetration of the illicit activity according to the section 54 of the Cybercrimes Act. Lastly, the Act lacked specifically regarding the type of assistance a financial institution should provide, the duration for the data retention by these institutions or service providers, and the timeline for police response to a reported incident.

This study recommends the provision of laws that stipulate greater punishment for the threat actors to aid the fight against cyberfraud perpetration. The decision-makers, as part of the decision-making processes, must consider the viability of the internal control measures in their cyberfraud mitigation policy (Nasser, 2020). Furthermore, organisations must build capacities that can effectively handle the emerging technologies to mitigate cyberfraud. Business organisations may consider the development of robust internal controls and reinforce their security and cyber defence architecture as a way to strengthen the cyber infrastructure targeted by the threat actors and also educate their potential "victims" to prevent their vulnerability against cyberfraud. These strategies may disrupt the plans of the "potential offenders." Hence, human capacity development as well as sensitisation of customers and employees will be helpful.

Amongst others, the collaboration should encourage information exchange and specify the obligations of the parties, the cross-border impacts, as well as the processes needed to effect foreign resolution measures. To effectively tackle the identified causative and motivating factors, the South African banking industry, in collaboration with other stakeholders in cyberfraud mitigation, needs to deploy emerging anti-cyberfraud technologies, ensure cyber resilience, and strengthen their internal control architecture.

This study contributes theoretically and empirically to the existing knowledge of the impact of legislation on cybercrime mitigation. The in-depth literature review adds to the understanding of the probable causes of cyberfraud in South Africa and its impacts. This may assist the stakeholders in the review of existing regulatory policies and legislations to adequately address the dynamic and emerging trend of cyberfraud perpetration.

This study is limited to explanatory research, systematic literature review of existing literature, and a survey. Future studies can consider the investigation of the impact of both the legal and regulatory frameworks on the rate of cyberfraud perpetration in South Africa using the mixed-method approach comprising quantitative and qualitative research designs.

Funding: This study received no specific financial support.

Institutional Review Board Statement: Not applicable.

Transparency: The authors state that the manuscript is honest, truthful, and transparent, that no key aspects of the investigation have been omitted, and that any differences from the study as planned have been clarified. This study followed all writing ethics.

Competing Interests: The authors declare that they have no competing interests.

Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.

REFERENCES

- Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, 6(1), 1-12. <https://doi.org/10.5897/jiis2015.0089>
- Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using balance score card: A survey of literature. *Journal of Financial Crime*, 27(3), 945-958. <https://doi.org/10.1108/JFC-03-2020-0037>
- Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2023). Application of forensic accounting techniques in the South African banking industry for the purpose of fraud risk mitigation. *Cogent Economics & Finance*, 11(1), 2153412. <https://doi.org/10.1080/23322039.2022.2153412>
- Akinbowale, O. E., Klingelhöfer, H. E., Zerihun, M. F., & Mashigo, P. (2024). Development of a policy and regulatory framework for mitigating cyberfraud in the South African banking industry. *Heliyon*, 10(1), 1-17. <https://doi.org/10.1016/j.heliyon.2023.e23491>
- Akinbowale, O. E., Mashigo, P., & Zerihun, M. F. (2023). The integration of forensic accounting and big data technology frameworks for internal fraud mitigation in the banking industry. *Cogent Business & Management*, 10(1), 2163560. <https://doi.org/10.1080/23311975.2022.2163560>
- Allen, K. (2021). *South Africa lays down law on cybercrime*. Retrieved from <https://issafrica.org/iss-today/south-africa-lays-down-the-law-on-cybercrime>
- Anon. (2020). *The online research guide for your dissertation and thesis laerd dissertation [online] Dissertation.laerd.com*. Retrieved from <https://dissertation.laerd.com/>
- Assessment Capacities Projects (ACAPS). (2012). *Qualitative and quantitative research techniques for humanitarian needs assessment an introductory brief*. Retrieved from <https://reliefweb.int/>
- Barlow, B. (2023). *What makes SA a target for cyber crime, what actions can be taken?* Retrieved from <https://www.itweb.co.za/content/Pero37Z34ydmQb6m>
- Bentouhami, H., Casas, L., & Weyler, J. (2021). Reporting of “theoretical design” in explanatory research: A critical appraisal of research on early life exposure to antibiotics and the occurrence of asthma. *Clinical Epidemiology*, 27(13), 755-767. <https://doi.org/10.2147/clep.s318287>
- Cassim, F. (2011). Addressing the growing spectre of cyber crime in Africa: Evaluating measures adopted by South Africa and other regional role players. *Comparative and International Law Journal of Southern Africa*, 44(1), 123-138.
- 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/Potchefstroomse Elektroniese Regsblad*, 24(1), 1-33. <https://doi.org/10.17159/1727-3781/2021/v24i0a10742>
- Clarke, R. V., & Felson, M. (1993). *Routine activity and rational choice* (Vol. 5). New Brunswick, NJ: Advances in Criminological Theory.
- CMS Law. (2024). *Understanding South Africa's Cybercrimes act*. Retrieved from <https://cms-lawnow.com/en/ealerts/2024/07/understanding-south-africa-s-cybercrimes-act?format=pdf&v=10>

- Coetzee, J. (2018). Strategic implications of fintech on South African retail banks. *South African Journal of Economic and Management Sciences*, 21(1), 1-11. <https://doi.org/10.4102/sajems.v21i1.2455>
- Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44, 588-608. <https://doi.org/10.2307/2094589>
- Cornish, D., & Clarke, R. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology*, 25(4), 933-947. <https://doi.org/10.1111/j.1745-9125.1987.tb00826.x>
- Dagada, R. (2013). *Digital banking security, risk and credibility concerns in South Africa*. Paper presented at the Proceedings of the Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013) Kuala Lumpur, Malaysia, 4 - 6 March 2013.
- Daniyan, I., Mpofu, K., Ramatsetse, B., & Gupta, M. (2021). Review of life cycle models for enhancing machine tools sustainability: Lessons, trends and future directions. *Heliyon*, 7(4), 1-21. <https://doi.org/10.1016/j.heliyon.2021.e06790>
- Dlamini, S., & Mbambo, C. (2019). Understanding policing of cybe-rcrime in South Africa: The phenomena, challenges and effective responses. *Cogent Social Sciences*, 5(1), 1675404. <https://doi.org/10.1080/23311886.2019.1675404>
- Dlamini, Z., & Modise, M. (2012). *Cyber security awareness initiatives in South Africa: A synergy approach*. Paper presented at the 7th International Conference on Information Warfare and Security, Seattle, USA, pp.1-10.
- Du Toit, R., Hadebe, P. N., & Mphatheni, M. (2018). Public perceptions of cybersecurity: A South African context. *Acta Criminologica: African Journal of Criminology & Victimology*, 31(3), 111-131.
- Dzomira, S. (2015). Online & electronic fraud prevention & safety tips cognizance in South African banks. *Socioeconomica-Naučni Casopis za Teoriju i Praksu Društveno-Ekonomskeg Razvoja*, 4(8), 527-540. <https://doi.org/10.12803/sjseco.48131>
- Dzomira, S. (2017). Internet banking fraud alertness in the banking sector: South Africa. *Banks & Bank Systems*(12,№ 1 (cont.)), 143-151. [https://doi.org/10.21511/bbs.12\(1-1\).2017.07](https://doi.org/10.21511/bbs.12(1-1).2017.07)
- Enofe, A. O. U., O., & Danjuma, E. (2015). The role of forensic accounting in mitigating financial crimes. *International Journal of Commerce and Management Research*, 1(1), 40-47.
- Gottschalk, P. (2010). Categories of financial crime. *Journal of Financial Crime*, 17(4), 441-458. <https://doi.org/10.1108/13590791011082797>
- Government Gazette Republic of South Africa. (2002). Electronic communication and transaction act. 446(23708), 1-80. https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf
- Graham, E. G., & Bennett, S. (2013). *Community policing in indigenous communities*. CA: Wadsworth.
- Grobler, M., Van Vuuren, V. J., & Zaaiman, J. (2013). Preparing South Africa for cyber crime and cyber defense. *Systemics Cybernetics and Informatics*, 11(7), 32-41.
- Grobler, T., & Louwrens, C. P. (2009). High-level integrated view of digital forensics. In (pp. 1-20). Johannesburg: University of Johannesburg.
- Gumbi, D. (2017). *Understanding the threat of cybercrime: A comparative study of cybercrime and the ICT legislative Frameworks of South Africa, Kenya, India, the United States and the United Kingdom*. LLM Degree Thesis in Commercial Law, University of Cape Town.
- Hasham, S., Joshi, S., & Mikkelsen, D. (2019). *Financial crime and fraud in the age of cybersecurity*. Retrieved from <https://www.mckinsey.com/~media/McKinsey/Business%20Functions/Risk/Our%20Insights/Financial%20crime%20and%20fraud%20in%20the%20age%20of%20cybersecurity/Financial-crime-and-fraud-in-the-age-of-cybersecurity.pdf>
- Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, 30(1), 1-25. <https://doi.org/10.1080/01639620701876577>
- Hopkin, P. (2010). *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management*. London: Kogan Page Limited.
- Information Security Institute. (2013). *Impact of cybercrime*. Retrieved from <https://resources.infosecinstitute.com/topic/2013-impact-cybercrime/>

- International Finance Corporation. (2020). *E-conomy Africa 2020 Africa's \$180 billion internet economy future*. Retrieved from <https://www.ifc.org/wps/wcm/>
- INTERPOL. (2021). *Africa's cyberthreat assessment report: INTERPOL'S key insight to cybercrime in Africa*. Retrieved from <https://www.interpol.int/en/>
- INTERPOL. (2024). *African cyberthreat assessment report 2024 outlook by the African cybercrime operations desk INTERPOL*. Retrieved from https://www.interpol.int/content/download/21048/file/24COM005030-AJFOC_Africa%2520Cyberthreat%2520Assessment%2520Report_2024_complet_EN%2520v4.pdf
- INTERPOL Report. (2022). *South Africa is the cybercrime hub of Africa, according to INTERPOL*. Retrieved from <https://techcabal.com/2023/04/19/south-africa-interpol-cybercrime/>
- Joel, C., & Vyas-Doorgapersad, S. (2019). An analysis of risk management within the department of trade and industry. *Journal of Contemporary Management*, 16(1), 357-375. <https://doi.org/10.35683/jcm192.0018>
- Juran. (2019). *Quality 4.0: The future of quality?* Retrieved from <https://www.juran.com/blog/quality-4-0-the-future-of-quality/>
- Kshetri, N. (2015). Cybercrime and cybersecurity issues in the BRICS economies. *Journal of Global Information Technology Management*, 18(4), 245-249. <https://doi.org/10.1080/1097198x.2015.1108093>
- Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, 22(2), 77-81.
- Lakshmi, P., & Menon, G. (2016). Forensic accounting: A checkmate for corporate fraud. *Journal of Modern Accounting and Auditing*, 12(9), 453-460. <https://doi.org/10.17265/1548-6583/2016.09.002>
- Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, 37(3), 263-280. <https://doi.org/10.1080/01639625.2015.1012409>
- Louw, D. (2012). *Mentoring children guilty of minor first-time crime: Methods, strength and limitations* (5th ed.). Bloemfontein: SA Publication.
- Mandia, K. (2011). *Incident response investing computer crime*. Osborne, CA: McGraw-Hill Press.
- Maware, C., Muvunzi, R., Machingura, T., & Daniyan, I. (2024). Examining the progress in additive manufacturing in supporting lean, green and sustainable manufacturing: A systematic review. *Applied Sciences*, 14(14), 6041. <https://doi.org/10.3390/app14146041>
- Mbelli, T. M., & Dwolatzky, B. (2016). *Cyber security, a threat to cyber banking in South Africa: An approach to network and application security*. Paper presented at the Proceedings of the 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing, pp.1-6.
- McEwan, T. E., Mullen, P. E., & MacKenzie, R. (2010). Suicide among stalkers. *Journal of Forensic Psychiatry and Psychology*, 21, 514-520.
- McIntyre, J.-L., Van Graan, C., Van Romburgh, J., & Van Zyl, A. (2014). Contextualizing the South African forensic accountant. *Journal of Forensic & Investigative Accounting*, 6(3), 98-122.
- Mehta, A., & Bhavani, G. (2017). Application of forensic tools to detect fraud: The case of Toshiba. *Journal of Forensic and Investigative Accounting*, 9(1), 692-710.
- Mittal, P., Kaur, A., & Gupta, P. K. (2021). The mediating role of big data to influence practitioners to use forensic accounting for fraud detection. *European Journal of Business Science and Technology*, 7(1), 47-58. <https://doi.org/10.11118/ejobsat.2021.009>
- Modugu, K. P., & Anyaduba, J. (2013). Forensic accounting and financial fraud in Nigeria: An empirical approach. *International Journal of Business and Social Science*, 4(7), 281-289.
- Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People*, 7(1), 23-48. <https://doi.org/10.26458/jedep.v7i1.571>
- Mohammed, H. K., & Knapkova, A. (2016). The impact of total risk management on company's performance. *Procedia-Social and Behavioral Sciences*, 220, 271-277. <https://doi.org/10.1108/ijqrm-07-2014-0090>

- Mohd-Sanusi, Z., Mohamed, N., Omar, N., & Mohd-Nassir, M.-D. (2015). Effects of internal controls, fraud motives and experience in assessing likelihood of fraud risk. *Journal of Economics, Business and Management*, 3(2), 194-200. <https://doi.org/10.7763/joebm.2015.v3.179>
- Mushtaque, K., Ahsan, K., & Umer, A. (2015). Digital forensic investigation models: An evolution study. *JISTEM-Journal of Information Systems and Technology Management*, 12, 233-243. <https://doi.org/10.4301/s1807-17752015000200003>
- Nasser, A. (2020). Cybercrime: theoretical determinants, criminal policies, prevention & control mechanisms. *International Journal of Technology and Systems*, 5(1), 34-63. <https://doi.org/10.47604/ijts.1133>
- Oguda, N. J., Albert, O., & Byaruhanga, J. (2015). Effect of internal control on fraud detection and prevention in district treasuries of Kakamega County. *International Journal of Business and Management Invention*, 4(1), 47-57.
- Oppenheim, A. N. (1992). *Questionnaire design, interviewing and attitude measurement*. London: Pinter.
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., . . . Brennan, S. E. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372.
- Shahbuddin, A., Alam, A., & Azad, M. (2011). Internal control in management information system. *International Journal of Computer Informations*, 2(6), 68-78.
- Shimoli, D. (2015). Forensic accounting: Signaling practicing accountants to improve skillset and forming regulatory body for forensic accountants in India. *Global Journal for Research Analysis*, 4(5), 63-66.
- Snail ka Mtuze, S., & Musoni, M. (2023). An overview of cybercrime law in South Africa. *International Cybersecurity Law Review*, 4(3), 299-323. <https://doi.org/10.1365/s43439-023-00089-8>
- Surendran, A. (2019). *Quantitative research: Definition, methods, types and examples*. Retrieved from https://www.questionpro.com/blog/quantitativeresearch/#Quantitative_Research_Examples
- Surfshark. (2022). *South Africa ranked 5th on global cybercrime density list*. Retrieved from <https://www.itweb.co.za/content/KA3WwMdz1nBvrydZ>
- Sutherland, E. (2017). Governance of cybersecurity-the case of South Africa. *The African Journal of Information and Communication*, 20, 83-112. <https://doi.org/10.23962/10539/23574>
- The South African Government. (2021). *Cybercrime act19 of 2020 (English/Afrikaans)*. Retrieved from <https://www.gov.za/documents/acts/cybercrimes-act-19-2020-english-afrikaans-01-jun-2021>
- Wilson, N., & McClean, S. (1994). *Questionnaire design: A practical introduction university of Ulster copies available from: UCoSDA, Level Six, university house*. University of Sheffield: Sheffield S10 2TN.

Views and opinions expressed in this article are the views and opinions of the author(s), International Journal of Management and Sustainability shall not be responsible or answerable for any loss, damage or liability etc. caused in relation to/arising out of the use of the content.