Akinbowale, Oluwatoyin Esther; Klingelhöfer, Heinz Eckart; Zerihun, Mulatu Fekadu

Article

Application of forensic accounting techniques in the South African banking industry for the purpose of fraud risk mitigation

Cogent Economics & Finance

Provided in Cooperation with:
Taylor & Francis Group

Suggested Citation: Akinbowale, Oluwatoyin Esther; Klingelhöfer, Heinz Eckart; Zerihun, Mulatu Fekadu (2023) : Application of forensic accounting techniques in the South African banking industry for the purpose of fraud risk mitigation, Cogent Economics & Finance, ISSN 2332-2039, Taylor & Francis, Abingdon, Vol. 11, Iss. 1, pp. 1-21, https://doi.org/10.1080/23322039.2022.2153412

Cogent Economics & Finance

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/oaef20

Application of forensic accounting techniques in the South African banking industry for the purpose of fraud risk mitigation

Oluwatoyin Esther Akinbowale, Heinz Eckart Klingelhöfer & Mulatu Fekadu Zerihun

To cite this article: Oluwatoyin Esther Akinbowale, Heinz Eckart Klingelhöfer & Mulatu Fekadu Zerihun (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, DOI: 10.1080/23322039.2022.2153412

To link to this article: https://doi.org/10.1080/23322039.2022.2153412

Published online: 16 Feb 2023.

cogent economics & finance

FINANCIAL ECONOMICS | RESEARCH ARTICLE

Application of forensic accounting techniques in the South African banking industry for the purpose of fraud risk mitigation

Oluwatoyin Esther Akinbowale[1]*, Heinz Eckart Klingelhöfer[1] and Mulatu Fekadu Zerihun[1]

Received: 30 July 2022
Accepted: 27 November 2022

*Corresponding author: Oluwatoyin Esther Akinbowale, Faculty of Economics & Finance, Tshwane University of Technology, Pretoria, South Africa
E-mail: Oluwatee01@gmail.com

Reviewing editor:
David McMillan, University of Stirling, Stirling, United Kingdom

Additional information is available at the end of the article

Abstract: The purpose of this study is to investigate the application of forensic accounting techniques in relation to fraud risk mitigation. This study employed an explanatory research design and a qualitative approach accompanied with a purposive sampling method. A primary data source was devised with a focus on the 17 licensed commercial banks registered in South Africa. By obtaining a true reflection of the situations in the banks, a conclusion was drawn following the outcome of the inferential statistical analysis. The research was conducted at the individual and organisational levels, with the bank consultants presenting their views. One hypothesis was formulated and non-parametric statistical analyses involving the use of Chi-square test, Fisher's Exact test and Spearman's correlation were carried out. The results obtained substantiate that the loopholes created as a result of non-effective application of forensic techniques are partly responsible for some cyberfraud incidents in the banking industry. There is no sufficient evidence to ascertain whether the fraud risk assessment and management in the banking industry has a relationship with the effective application of forensic accounting techniques in terms of the identified causes of cyberfraud. However, the findings establish a positive correlation between fraud risk assessment and management as

ABOUT THE AUTHORS

Oluwatoyin Esther Akinbowale is a Postdoctoral Research Fellow at the Faculty of Economics and Finance, Tshwane University of Technology, Pretoria, South Africa. Her research interests include forensic accounting, management accounting, management information system, accounting information system as well as financial reporting.
Heinz Eckart Klingelhöfer is a Professor for Managerial Accounting and Finance in the Department of Finance and Investment, Tshwane University of Technology, Pretoria, South Africa.
Mulatu Fekadu Zerihun is a Professor and the Head of Department of Economics. He has published widely in areas related to open economy macroeconomics, development economics, and environmental economics.

PUBLIC INTEREST STATEMENT

The banking industry is faced with increasing cyberfraud risk with the use of emerging technologies and digital platforms for banking. This has negative impacts on customers' satisfaction, profitability, goodwill and reputation of the banking industry. However, the effective application of forensic accounting is one of the approaches to mitigate cyberfraud related risks. Hence, this study investigates the application of forensic accounting techniques in the South African banking industry vis-à-vis fraud risk assessment and management. The findings substantiate the fact that the loopholes created by non-effective application of forensic techniques are partly responsible for some cyberfraud incidents in the banking industry. This study provides an insight into the significance of the application of forensic accounting for fraud risk minimisation. Since there is still a death of information regarding forensic accounting for fraud risk mitigation, it is envisaged that this study will add to the existing literature in this regard.

cogent • economics & finance

it relates to forensic accounting implementation. This study provides an insight into the significance of forensic accounting applications for fraud risk mitigation. There is still a death of information regarding the forensic accounting for fraud risk mitigation; hence, it is envisaged that this study will add to the existing literature in this regard.

Subjects: Economics; Finance; Business, Management and Accounting

Keywords: Cyberfraud; Forensic accounting; Information security; Management control systems

1. Introduction

According to Mishkin and Serletis (2011:5), "banks are financial institutions that accept deposits and make loans." It comprises firms such as the chartered banks, trust and mortgage loan corporations, as well as credit unions and *caisses populaires* (Mishkin & Serletis, 2011:5). The banking industry can be seen as a vital industry to the economy through fiscal and monetary policy formulation, credit facilities and regulation of cash flows (Wright, 2011:13–54). This study has theoretical importance as well as empirical applications in the areas of business operations and policymaking. The South African banking industry can modify its practices to combat cyberfraud as well as to identify areas of deficiency in this regard. Furthermore, by highlighting the problems that banks experience within the South African banking system, relevant information is provided for regulators on how the regulation of banking institutions can be improved to mitigate the effect of cyberfraud on the South African economy.

Forensic accounting focuses on fraud risk management. That is, it facilitates the assessment of all the risks associated with an organisation including fraud risk (Chih-Hao & Kuen-Chang, 2020:3). In addition, it ensures that the risks capable of hindering the actualisation of an organisation´s goals are put under control (Shah et al., 2011:537). Forensic accounting can contribute to understanding the general conditions that permit the occurrence of fraud, working with the concept of cause and effect (Santos Filho et al., 2017:70). Previous studies were carried out by scholars of fraud and the commercial banking industry. For instance, Wanemba (2010:30) established the challenges of fraud confronted by commercial banks in Kenya and identified strategies that banks employ to combat fraud. The study was carried out because of the need for commercial banks to respond felicitously to the challenge of fraud mitigation. The outcome highlighted five key challenges that banks are facing: irregular, unusual transaction monitoring and reporting, advancement in technology, authentication of account documents, application of corporate policy or code of conduct, and adequate background checks not performed on new employees.

The overall objective of this study is to examine the application and the effectiveness of forensic accounting techniques in the South African banking industry with respect to fraud risk assessment and management. First, the possible causes of cyberfraud were investigated, and the relationship between effective application of forensic accounting techniques in terms of the identified causes of cyberfraud was investigated. Secondly, the relationship between fraud risk assessment and management as it relates to forensic accounting implementation was ascertained.

This study provides an insight into the significance of the application of forensic accounting for fraud risk minimisation. Since there is still a death of information regarding forensic accounting for fraud risk mitigation, it is envisaged that this study will add to the existing literature in this regard. The rest of the paper is organised as follows: the second section presents the literature review, this is followed by the methodology in the third section, results and discussion in the fourth section and the last section presents the conclusion drawn from the findings vis-à-vis the objectives as well as recommendations and policy framework.

2. Literature review

The literature in this section comprises an overview of the structure of the South African banking industry, the views of various scholars, forensic accounting, and fraud risk management practices.

2.1. The South African banking industry

The South African banking industry is well developed in Africa and is comparable in sophistication to the financial industries in most developed countries (Moyo, 2018:3; South African Banking South African Banking Report, 2019). The sector is managed, regulated and controlled by the South African Reserve Bank, which ensures the soundness and safety of its systems (South African Reserve Bank (SARB), 2020). This means that the banks are regulated from a common platform with the aim to achieve a robust banking system in the interest of the customers and the economy in accordance with the Banks Act (No. 94 of 1990) or the Mutual Banks Act (No. 124 of 1993; South African Reserve Bank (SARB), 2020).

According to the South African Reserve Bank, 75 banks are operating commercially. Of these, there are three mutual banks, six foreign controlled banks, 42 foreign bank representatives, 14 branches of foreign banks and 10 banks that are locally managed (South African Reserve Bank (SARB), 2020). However, the sector is dominated by the five biggest banks in the country, accounting "for over 90% of the total banking assets in the country, valued at approximately R5.8 trillion." (BusinessTech, 2021). Factors like digital solutions, cost-effective operating models and supply-chain integration have moved to the top of the business agenda, with non-traditional players pursuing various aspects of these trends, thereby ensuring the provision of in-house banking solutions to customers (PwC Report, 2019:6). This means that with regard to the rising risk of cyberfraud in the retail banking industry, the traditional banks need to find new ways to facilitate a consistent relevance in the market, prioritising main operational trends like digital transformation and data mining (PwC Report, 2019:9).

2.2. The concept of forensic accounting

The aim of forensic accounting is identifying fraudulent activities both inside and outside an organisation with its own models, methodologies and procedures of investigation that enquires for assurance, attestation, and advisory standpoint to produce comprehensive legal evidence (Modugu & Anyaduba, 2013:287). Forensic accounting is an incorporation of accounting principles, investigative techniques, legal procedures, and accounting skills in gathering financial information that would serve as evidence and will be acceptable in the court of law during the resolution of fraud-related matters (Wells, 2003:76; Houck et al., 2006:68; Bassey & Ahonkhai, 2017:57). The aspects of the inquiry in forensic accounting are extensive and comprise fraud examination, comprehensive diligence reviews, risk assessment, detection of financial statement misrepresentation, cybercrimes, and unlawful money transfers (Smith & Crumbley, 2009:66; Okoye & Gbegi, 2013:135).

The process of investigating suspected cyber-fraud is called digital forensic investigation/accounting. This is defined as an enquiry into suspected fraud cases, which occurred through the internet or via an intrusion into the organisation's computer system. The digital forensics comprise the processes of discovery, acquiring and investigating information connected to digital devices that can store information in the digital form (Brown, 2015:72). The validity of any digital forensic evidence for litigation purposes depends on the strict adherence to the set of guidelines during the processes of data collection and analysis both before and during the investigation process (Ayers et al. (2014:68). Hence, forensic accounting software is often used to ensure that the data analysis process is completed in a time effective manner and at a higher confidence level, although the forensic investigator may employ different techniques depending on the nature of the data acquired and the information required (Albano et al., 2011:381).

The use of reliable digital forensic techniques is central to fraud detection, prevention, investigation, and reporting (Nissan, 2012:843). Digital forensic investigations can be proactive or reactive in nature. Proactive digital forensics is described as the process of restructuring, procedure description and technology to create, collect, preserve, and manage comprehensive digital evidence in order to ensure a successful and inexpensive investigation with minimal disruption of business activities whilst demonstrating good governance. On the other hand, reactive digital forensic is defined as an investigation that takes place after an incident has been detected. It is embodied with the goals to ascertain the root-cause of the incident, link the perpetrator to the incident, minimize the impact of an incident and successfully investigate an incident. However, should an incident occur, there should be an acceptable recognised digital forensic investigation procedure in place as specified by proactive digital forensics discussed above (Vonsolms et al., 2006:348). Rowlingson (2004:9) describes 10 key activities necessary for the implementation of a forensic program. These are:

- definition of the business situations that require digital evidence,
- identification of the available sources and various types of potential evidence,
- determination of the requirements for evidence collection,
- establishment of the capability for gathering digital evidences legally such that they will be admissible as evidence during the litigation process,
- establishment of a policy for safe storage and handling of potential or captured evidence,
- effective monitoring to detect and deter major incidents,
- specification of the circumstances in which the digital evidence may be launched for full investigation,
- staff training on incident awareness and sensitivities of evidence from the legal perspectives,
- documentation of an evidence-based case that describes the incident and its impact, and
- provision of legal review to facilitate effective response to the incident.

In terms of fraud mitigation, Enofe et al. (2013:68) revealed that the act of mitigating corporate crime could be attained by devoting strength to corporate governance through forensic accounting. Cusack and Ahokov (2016:17), in their study on the investigation of the performance of forensic software tools in detecting fraud detection, stated that the use of FA techniques for mitigating fraud is necessary because most information relating to accounting is currently in digital form coupled with dimensions that digital fraud is assuming. The authors emphasise that the rate of fraud perpetration is increasing and proof of fraud incidents are becoming increasingly complex compared to the past decades.

Thus, previous studies have established that FA plays a major role in fraud detection and prevention in corporate organisations (Efosa & Kingsley, 2016:245; Peshori, 2015:35; Enofe et al., 2013:68; Okoye & Gbegi, 2013:1).

2.3. Fraud risk management in the banking industry

Stoneburner et al. (2002:8) defines risk as the probability that a threat source will adversely impact an organisation. Risk management can be defined as a vital part of a financial institution's strategic decision-making process that ensures that its corporate objectives are consistent with an appropriate risk return trade-off (Hopkin, 2010:47; Boateng et al., 2014:43). In the opinion of Kopp et al. (2017:8), effective risk management at various levels is a collective responsibility of all the organisation's stakeholders. Fraud risk management refers to the activities aimed at identifying and developing actions for a business to mitigate risks arising from the actual and potential cases of corporate fraud. It includes the preventive, corrective, directive and detective control measures with the appropriate feedback where necessary (Hopkin, 2010:255).

Combining the works of Hopkin (2010:3) and Stoneburner et al. (2002:4), risk management involves systematic processes of risk identification, assessment, control, and evaluation. Fraud identification is linked with fraud detection whereby activities are carried out to ascertain a potential fraud or fraudulent activities immediately they occur (KPMG, 2010:24). The assessment is basically to investigate the cost, extent, and impact of such risk on the customers, organisation, general public and stakeholders, while the fraud control involves series of activities, which can either be proactive or reactive in nature to a potential risk, while the evaluation phase is to investigate the effectiveness of the measures deployed in all the preceding stages of risk management.

Banks are confronted with various risks, such as interest rate risk, market risk, credit risk, off balance-sheet risk, technology and operational risk, foreign exchange risk, country or sovereign risk, liquidity risk, liquidity risk and insolvency risk (Saunders & Cornett, 2017:177–193).

Aldasoro et al. (2022:11) explain that the digital revolution has improved the connectivity and intricacy of the economic system. The authors identified the use of the cyber space and emerging technologies as major contributors to an organisation's productivity. However, the exploitation of the cyber space and the emerging technologies by the cyber attackers have also exposed the financial institutions to cyberattacks.

In an attempt to assess cyber risk, Giudici & Raffinetti (2022:1325) developed an artificial intelligence (AI) model that integrates the rank regression and Lorenz Zonoids models. The outcome of the study demonstrates the applicability of the machine learning approach for the assessment of cyber risk. The outcome also indicates that the integration of the two approaches is suitable for the measurement of ordinal measurement variables during cyber risk assessment. The implementation of the proposed models led to the identification of the drivers of cyber risk, which are necessary for the mitigation of cyber risks.

Radanliev et al. (2018:21) as well as Ruan (2017:17) demonstrated the suitability of combining the Cyber Value-at-Risk (CyVaR) model and MicroMort (MM) for calculating risk indices and establishing an acceptable level for IoT-based cyber-related risks. The outcomes of these studies promote the efforts geared towards the integration of cyber risk impact assessments, thus offering a better understanding of the economic impact assessment of IoT-based cyber-related risks.

Shin et al. (2015) employed the Bayesian networks to integrate two cyber security risk models. The first model was suitable for the assessment of people's and organisations' compliance to the cyber security guidelines, while the second model investigates the probability of cyberattack on the architecture of the reactor protector's system.

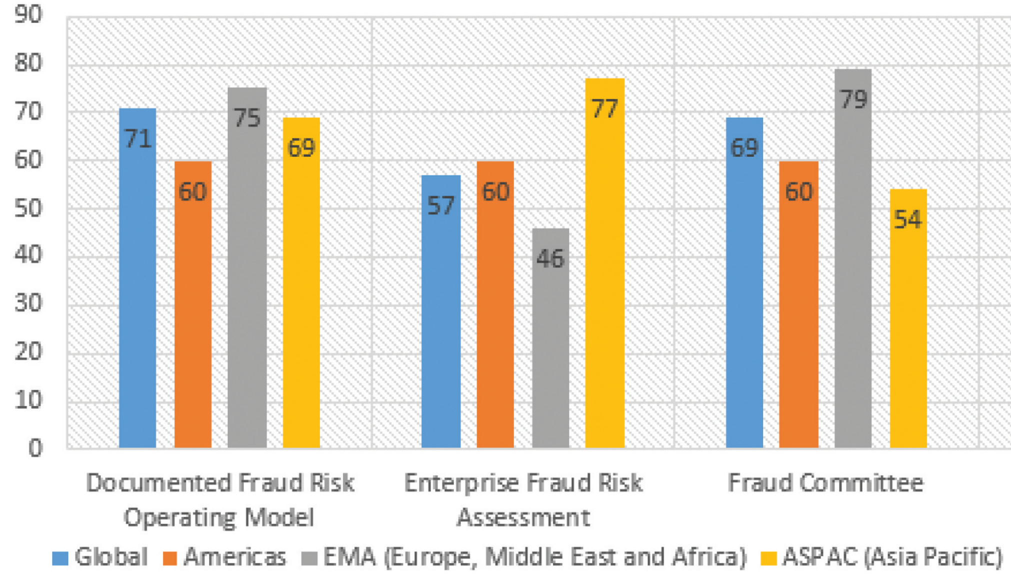
The effective management of these risks is essential to a bank's performance. However, according to the taxonomy of risks developed by Leo et al. (2019:4), fraud risk is classified under operational risk. This is because operational risk is a risk of losses, which could stem from either the failure of internal systems or external occurrences (Leo et al., 2019:3).

Fraud risk management becomes an incomplete exercise without fraud control. Fraud control is the measure put in place to guide against deviations from normal activities and correct suspected cases of irregularities in the financial statement. Without effective fraud control measures, fraudulent behaviours will increase with an increase in substantial losses (Hopkin, 2010:236). Fraud control can be preventive (pre-control process) and detective (post-control process), these two processes have a common channel, which is investigation (Hopkin, 2010:255). However, before implementing any control techniques, the risk associated must be identified and dealt with accordingly. Furthermore, to avoid post-fraud control processes, risk assessment must be thorough and effective.

As depicted in Figure 1, the survey carried out by KMMG in 2019 found that not all the respondents have a recorded fraud risk management operating model, therefore an initiative-wide fraud risk assessment was conducted.

Figure 1. Wide fraud risk assessment and response rate.

Source: KPMG (2019:16)



2.4. Derivation of research hypothesis

As indicated in the works of Henderson and Greaves (2011:320) and Lueg and Knapik (2016:78) the right application of forensic accounting can aid the process of fraud mitigation, risk assessment and management. Chih-Hao and Kuen-Chang (2020:3) opine that forensic accounting is focused on fraud risk management, that is, it facilitates the assessment of all the risks associated with an organisation including fraud risk. This ensures that the risks capable of hindering the actualisation of an organisation goal are put under control (Shah et al., 2011:537). Based on this premise of the literature reviewed, one alternative hypothesis is considered in this study as follows:

H_1: *Fraud risk assessment and management in the banking industry have a relationship with the effective application of forensic accounting techniques.*

Recall that the overall objective of this study is to examine the application and the effectiveness of forensic accounting techniques in the South African banking industry with respect to fraud risk assessment and management. To achieve this objective the possible causes of cyberfraud were identified. Thereafter, the relationship between effective application of forensic accounting techniques in terms of the identified causes of cyberfraud was investigated. Furthermore, the relationship between fraud risk assessment and management as it relates to forensic accounting implementation was ascertained.

3. Data and methodology

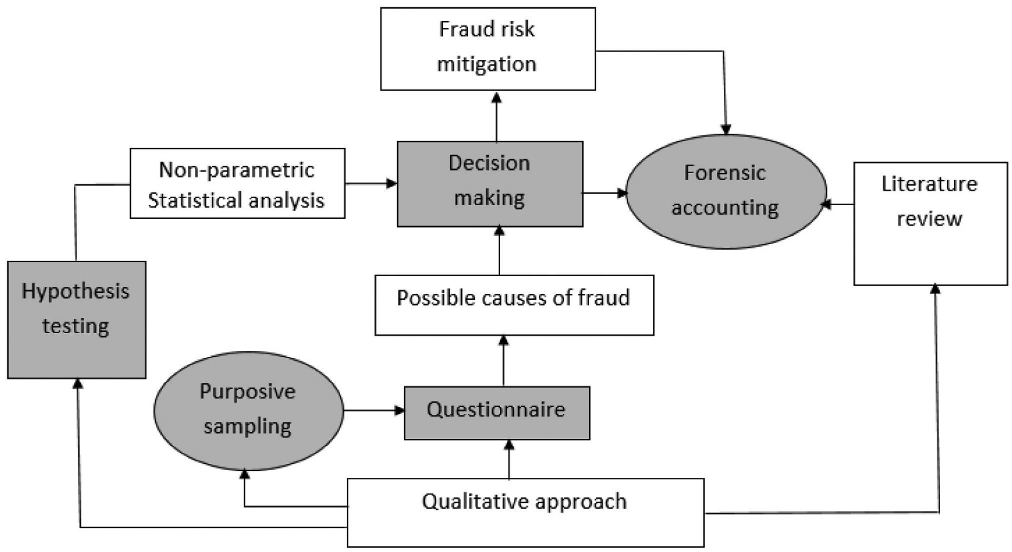
This study employed an explanatory research design, accompanied by a qualitative approach involving a purposive sampling method (Figure 2).

A primary data source was devised with a focus on the 17 licensed commercial banks in South Africa (Bankscope, 2018).

This study employs questionnaires as a primary data collection method due to their capability to capture and verifies sensitive issues like cyberfraud in a standardised manner, making them objective (Oppenheim, 1992; Wilson & Mcclean, 1994). The data garnered help to ensure a confirmatory outcome and avoid a biased point of view. The questionnaires were administered to key organisational staff across the banking industry, specifically involved in combating fraud

Figure 2. Research design.

Source: Authors'



and making decisions regarding management control systems, to obtain comprehensive information on the organisation's expended and ongoing efforts to combat cyberfraud.

The qualitative approach employed presents the opinions, concepts, characteristics and descriptions of different respondents (Jackson et al., 2007:22; Assessment Capacities Projects (ACAPS), 2012:13), as it relates to cyberfraud in this study. The choice of the qualitative approach in this study was based on the following merits: it can explore the research problem from the perspectives of the stakeholders and assist in the understanding of multifaceted or complex occurrences (such as cyberfraud) which is difficult to understand via a quantitative survey. Furthermore, it can simplify a complex problem to a number of variables and establish the correlation relationships between the variables. In addition, it is suitable for establishing the cause and effect relationships and also suitable for hypothesis testing, because it assumes a sample that is usually illustrative of the population. With this, general conclusions can be drawn for the population (Ospina, 2004:1279; Mohajan 2018:21).

The analysis carried out include non-parametric statistics (due to the categorical data from a limited sample size, obtained without a known distribution; Kampen & Swyngedouw, 2000:91; Wilson, 1977: 136), inferential univariate and multivariate inferential statistics (These methods include the cross tabulation, the Chi-square statistical analysis, Fisher's Exact test, and the Spearman correlation).

The expression of the chi-square employed for some inferential statistical analysis is given by Equation (1; Ugoni & Walker, 1995:62; Kim, 2017:153).

$$\chi 2 = \frac{(O-E)^2}{E} \tag{1}$$

where: O is the observed value of the cells and E the expected value.

The Fisher's Exact test values can be computed using Equation (2; Amigo-Dobaño et al., 2020:6).

$$p = \frac{(a+b)!(c+d)!(a+c)!(b+d)!}{a!b!c!d!N!} \tag{2}$$

where: $a, b, candd$ are the frequencies of the categorical variable of the 2×2 contingency table, while N is the total frequency.

The determination of the Spearman's correlation coefficient (ρ) can be obtained from Equation (3) for observations without ties (Chalil, 2000:14).

$$\rho = 1 - \frac{6 \sum d_i^2}{n^3 - n} \tag{3}$$

For observations with ties (which is our case), Equation (4) holds thus (Chalil, 2000:11).

$$\rho = \frac{\sum (X_i - X')(Y_i - Y')}{\sqrt{\sum (X_i - X')^2 . \sum (Y_i - Y')^2}} \tag{4}$$

where: d_i is the difference between each of the ranks of the corresponding values of the variables X and Y, and n is the number of pairs of values when there are no tied ranks.

According to Giudici & Raffinetti (2022:1319), the activities that characterise cyber events are unique. Coupled with non-availability data, it is more suitable to measure them using the ordinally scaled data rather than the quantitative data. The measurement of cyber risk using ordinally scaled data can be summarised, using a pair of statistics for each event type (Giudici & Raffinetti, :1319). This can aid the understanding of the major factors causing cyber risks, to avoid an arbitrary assignment of the measurement scale. This study explores the Chi-square statistical analyses, Fisher's exact test and Spearman's correlation for the hypothesis testing and for establishing the association between the identified variables relating to cyberfraud. The choice of these techniques for hypothesis testing stems from the fact that the data set employed in this study is not normally distributed.

4. Result and discussions

Of the initially planned sample of 68 individual respondents, only 42 questionnaires were administered and attended to—due to Covid_19 pandemic, huge load of work and reluctance to divulge confidential information—some bank officials did not give audience. Due to the Covid pandemic, the survey was limited to the licensed and available banks in Pretoria, South Africa, whose experts in cyberfraud mitigation gave audience to attempt the questions. However, the data obtained should still reflect the situation in the South African Banks since indeed *all* the 17 licensed banks (100%) were still covered and since there is a uniform system of standard operational procedur**es**, structure, regulation, and control in the South African banks under the auspices of the South African Reserve Bank. Furthermore, all the 42 questionnaires later administered were attended to. The fact that the responses obtained from the question asked were 100% indicates that there is no effect of the non-response bias on the outcome of the findings.

4.1. Hypothesis testing using the chi-square and the Fisher's exact tests

Under this subsection, the hypothesis considered in this study was tested using the Chi-square and the Fisher's exact tests on the qualitative responses obtained from the survey. Furthermore, the cross tabulation and the Spearman correlation coefficient were used to establish the nature of the relationship that exists between the pairs of variables used for the hypothesis testing. This is necessary in order to draw conclusions about the acceptance or rejection of the hypotheses. Below are the outcomes of the tests. The tests were conducted by coding and feeding in the qualitative responses obtained from the survey into the Statistical Package for Social Science (SPSS) 2018 version.

H_1: Fraud risk assessment and management in the banking industry have a relationship with the effective application of forensic accounting techniques

First, this hypothesis was tested using six variables for the possible causes of cyberfraud, linked to the process of fraud risk assessment and management (according to Brockett et al., 2012:324–336; Dzomira, 2015:9; Mohammed & Knapkova, 2016:271). These six variables are presented in Table 1. Secondly, having established the possible causes of cyberfraud in the South African banking sector, this study further probes whether the application of forensic accounting techniques can promote fraud risk assessment and management. This was investigated using the two variables (fraud risk assessment and fraud risk management) that link forensic accounting to the process of fraud risk mitigation.

Table 1 presents the Chi-square and Fisher's Exact tests for the possible causes of cyberfraud.

Two variables, namely override of internal controls by the management and inadequate documentation or record keeping, negate the alternative hypothesis tested since their p-values (0.069 and 0.092 for the chi-square test) and (0.071 and 0.091 for the Fisher's Exact test respectively) are greater than 0.05. The other four variables (poor organisational culture, lack of ethical culture, absence of accountability, installation and use of new technologies) support the acceptance of the alternative hypothesis since their p-values (0.000, 0.001, 0.000 and 0.005 for the chi-square test and 0.000, 0.001, 0.000 and 0.006 for the Fisher's Exact test respectively) are less than 0.05. Hence, from these findings, it could be substantiated that the loopholes created by non-effective application of forensic techniques are partly responsible for some cyberfraud incidents in the banking industry. However, there is no sufficient evidence to ascertain whether the fraud risk assessment and management in the banking industry has a relationship with the effective application of forensic accounting techniques in terms of the identified causes of cyberfraud.

Table 1. Chi-square and fischer's exact tests for the possible causes of cyberfraud

Identified possible causes of cyberfraud	Chi-square statistics	df	Asymp. Sig.	Fischer's Exact Sig.	Point probability
Overrides of internal controls by the management (OV)	8.714	4	0.069	0.071	0.007
Poor organisational culture (POC)	23.476	4	0.000	0.000	0.000
Lack of ethical culture (LEC)	18.714	4	0.001	0.001	0.000
Absence of accountability (AOA)	24.429	4	0.000	0.000	0.000
Inadequate documentation/ record keeping (ID)	8.000	4	0.092	0.091	0.005
Installation & use of new technology (INT)	10.429	2	0.005	0.006	0.001

Source: Field Survey

This calls for the need to introduce more anti-fraud capacities such as forensic accountants and preventive measures to meet the current demand in information technology and effective moderation of the internal control measures.

Table 2 shows the possible causes of cyberfraud in the South African banking industry. The largest percentage (91%) of the respondents agreed/strongly agreed that the installation and usage of new technology majorly causes cyberfraud, confirming existing literature (Dlamini et al., 2019:1; Herselman & Warren, 2004; Dzomira, 2017:143; Coetzee, 2018:3; Dagada, 20132013:148; Sutherland, 2017:84; Apau & Koranteng, 2019:229; Clough, 2010:209). Another critical factor identified as a major cause of cyberfraud, which a significant number of respondents acceded to, is the override of internal controls by the management. These findings significantly agree with the position of the American Institute of Certified Public Accountants (American Institute of Certified Public Accountants, AICPA, 2012) that the internal control measure is a major player in the detection and prevention of fraud, although the enforcement of internal controls alone may not be sufficient for fraud mitigation. This is due to the fact that internal controls can be weakened through collusion, management overrides and technological advances; hence, over-reliance on internal controls could jeopardise the fight against cyberfraud. The adoption of other measures was, however, recommended for effective fraud mitigation (American Institute of Certified Public Accountants (AICPA), 2012).

Furthermore, the respondents opined that poor organisation and lack of ethical culture are also part of the possible causes of cyberfraud. Good organisational culture can assist in the identification of the root causes of fraud perpetration and possible ways to mitigate its occurrence. Omar et al. (2013:230) indicate that forensic accountants should possess strong ethical values and skills to enable them perform optimally as fraud investigators. The consideration of ethical factors in the control systems may promote moral value behaviours of the employees. The respondents also identified the absence of accountability as one of the contributing factors to cyberfraud. To promote a good culture of accountability and transparency in the private and public sectors, Section 32(1) of the Constitution of the Republic of South Africa Act 108 of 1996 (the Constitution), provides that:

> "Everyone has the right of access to records or/and information held by the state and any information held by another person and that is required for the exercise or protection of any rights." (Promotion of Access to Information Act, 2020:2)

This section of the Constitution confirms the fundamental right of access to information and upholds the principle of accountability and transparency.

Finally, improper documentation was also identified as one of the possible causes of cyberfraud. It has been reported that weak internal controls can promote fraud perpetration as perpetrators can take undue advantage of internal control shortcomings such as poor supervision and improper document control processes to commit fraud (Dellaportas, 2013:29; Zakaria et al., 2016:1154; Andoh et al., 2018:411).

The identification of possible causes of cyberfraud calls for the need to establish or introduce more anti-fraud capacities and preventive measures to meet the current demand in information technology and effective moderation of the internal control measures.

Akinbowale et al. (2020a:945) suggested the need for the implementation of a real time alert system capable of creating fraud awareness for both the financial institutions and their customers. The development of forensic accounting conceptual models for cyberfraud uncovering and mitigation has also been reported Akinbowale et al. (2020b:1253).

Figure 3 presents the identified possible causes of cyberfraud from the survey carried out.

Table 2. Possible causes of cyberfraud

Possible causes of cyberfraud	No of response (n) Agree	No of response (n) Strongly Agree	No of response (n) Disagree	No of response (n) Strongly Disagree	No of response (n) Undecided	Total no of respondents (N)
Overrides of internal controls by the management	13	7	11	9	2	42
Poor organisational culture	11	2	16	11	2	42
Lack of ethical culture	7	2	17	13	3	42
Absence of accountability	6	7	14	14	1	42
Inadequate documentation/ record keeping	9	3	11	15	4	42
Installation & use of new technology	18	20	0	4	0	42

Source: Field Survey

Figure 3. The identified possible causes of cyberfraud.

Source: Survey

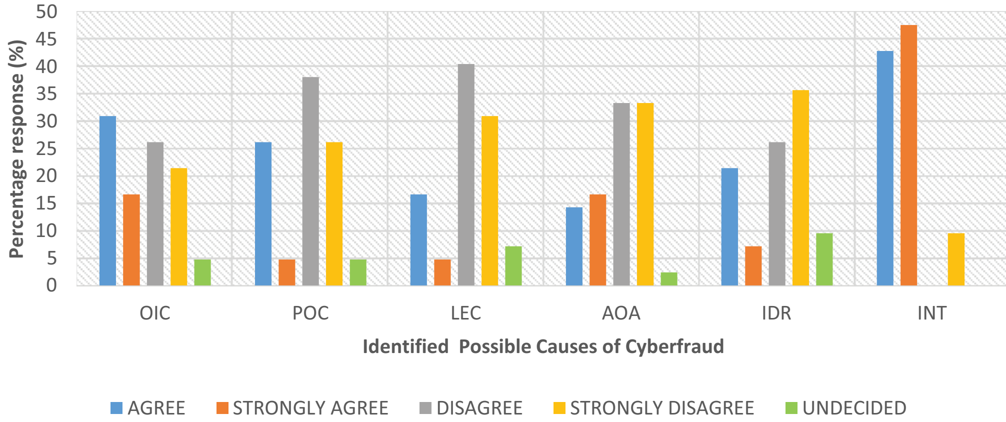


Table 3 presents the combination of the statistically significant factors (95% confidence level) that cause cyberfraud, confirming a relationship between the pairs of the variables in relation to cyberfraud perpetration.

The variable pairs are as follows: Poor Organisational Culture (POC) and Lack of Ethical Culture (LEC), Poor Organisational Culture (POC) and Absence of Accountability (AA), Lack of ethical culture (LEC) and absence of accountability (AA), Override of Internal Control (OIC) and Poor Organisational Culture (POC), Override of Internal Control (OIC) and Lack of Ethical Culture (POC), Override of Internal Control (OIC) and Absence of Accountability (AA), Override of Internal Control (OIC) and Inadequate Documentation and Record Keeping (IDR), as well as Inadequate Documentation and Record Keeping (IDR) and Installation and use of new technology (INT). The cross tabulation records the frequency of respondents that have the unique feature described in the cells of the table in order to establish a relationship between the variables.

For six pairs of variables, the difference between the observed and expected counts obtained from the cross-tabulation indicates that there may be a relationship between the following pairs of variables:

- poor organisation culture (POC) and lack of ethical culture (LEC)
- poor organisation culture (POC) and absence of accountability (AA)
- lack of ethical culture (LEC) and absence of accountability (AA)
- override of internal control (IOC) and poor organisation's culture (POC)
- lack of ethical culture (LEC) and override of internal control
- absence of accountability and override of internal control (IOC)

However, to determine whether the difference is statistically significant, the Spearman's correlation coefficient was calculated as presented in Table 3. According to this, there seems to be

- a positive and strong relationship between the variables LEC and AA, and
- a positive and moderate relationship between POC and LEC, POC and AA, OIC and POC, OIC and LEC as well as OIC and AA.

Also the Fisher Exact statistical values were large for the pairs of significant factors (p-values < 0.05); thus, the pair of variables can indeed be considered as dependent variables.

Based on the responses obtained, the cause effect diagram presented in Figure 4 depicts the possible causes of cyberfraud in the South African banking industry grouped into six major categories. The figure also shows the relationship between the causes of cyberfraud and the

Table 3. The statistical analysis of the possible causes of cyberfraud

Paired Factors	Fischer's Exact Test Statistics	df	Exact. Sig. (2 tailed)	Remarks	Spearman's Correlation Coefficient	Relationship
POC & LEC	64.770	16	0.000	• 23 cells (92.0%) have expected outcomes of less than 5. The minimum expected count is 0.05	0.542	Positive and moderate
POC & AA	30.158	16	0.001	• 23 cells (92.0%) have expected outcomes of less than 5. The minimum expected count is 0.02	0.545	Positive and moderate
LEC & AA	38.180	16	0.000	• 23 cells (92.0%) have expected outcomes of less than 5. The minimum expected count is 0.05	0.731	Positive and strong
OIC & POC	27.255	16	0.004	• 24 cells (96.0%) have expected outcomes of less than 5. The minimum expected count is 0.05	0.429	Positive and moderate

(*Continued*)

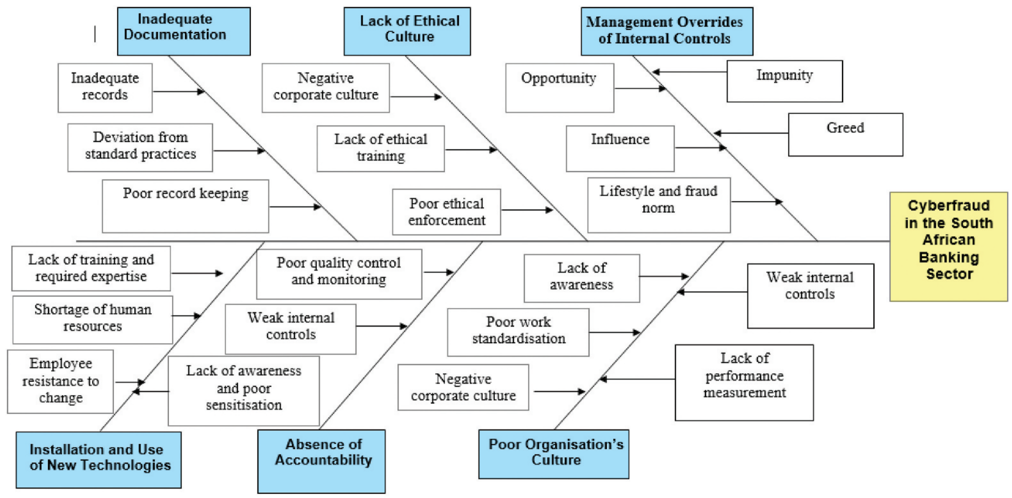
Table 3. (*Continued*)

Paired Factors	Fischer's Exact Test Statistics	df	Exact. Sig. (2 tailed)	Remarks	Spearman's Correlation Coefficient	Relationship
OIC & LEC	26.780	16	0.003	• 24 cells (92.0%) have expected out-comes of less than 5. The minimum expected count is 0.10	0.415	Positive and moderate
OIC & AA	28.358	16	0.002	• 24 cells (92.0%) have expected out-comes of less than 5. The minimum expected count is 0.05	0.524	Positive and moderate
OIC & ID	24.553	16	0.011	• 25 cells (100.0%) have expected out-comes of less than 5. The minimum expected count is 0.19	0.069	Positive but weak
ID & INT	13.993	8	0.034	• 12 cells (80.0%) have expected out-comes of less than 5. The minimum expected count is 0.57	0.174	Positive but weak

Source: Field Survey

Figure 4. Cause - effect diagram of the possible causes of cyberfraud.

Source: Authors'



influencing factors, hence, it may increase the understanding of cyberfraud with the aim of mitigating it.

Kshetri (2019:77) noted that the cases of cyberattacks on the emerging economies are rising, rapidly linking the probable causes to weak internal controls and emerging technologies as obtained in this study. Furthermore, Saddiq and Bakar (2019:911) stated that financial crimes have reportedly have an adverse effect on the economy and the socio-economic environment of both the emerging and advanced economies.

Although the findings in this study are based on the opinion of the bank consultants in South Africa, the provided results and solutions are not necessarily restricted to South Africa. Instead, cyberfraud being a digital problem that has assumed a global dimension and can be found in similar facets in many different countries, other financial institutions in other advanced and emerging economies may also implement the proposed solutions based on their peculiarities.

Having established the possible causes of cyberfraud in the South African banking sector, this study further probes whether the application of forensic accounting techniques can promote fraud risk assessment and management. Table 4 presents the results obtained with respect to this investigation. For fraud risk assessment, 80.95% of the total respondents agreed that the effective implementation of forensic accounting techniques can promote fraud risk assessment, while 14.28% respondents strongly agreed and only 4.76% respondents were undecided. For fraud risk management, 71.42% of the total respondents agreed that the effective implementation of forensic accounting techniques can promote for fraud risk management, while 19.05% respondents strongly agreed and only 9.52% respondents were undecided. The outcome of this survey indicated that none of the respondents opposed the fact that the effective application of forensic accounting can promote risk assessment and management. Figure 5 presents the cross-tabulation chart for fraud risk assessment and management with respect to effective forensic accounting applications.

The cross tabulation of the two variables, fraud risk assessment and management with respect to forensic accounting application, and the determination of the significance of their cross-effect yielded a Fisher's exact statistical value of 28.550 and a *p*-value less than 0.05 ($0.001>0.05$) at a 95% confidence level and four degrees of freedom. This means that there is a sufficient proof to establish that there is a relationship between the two variables. To establish the nature of relationship between the variables (fraud risk assessment and management with respect to forensic accounting application), the Spearman's non-parametric correlation was carried out and a correlation coefficient of 0.812 was obtained. A positive Spearman correlation coefficient implies

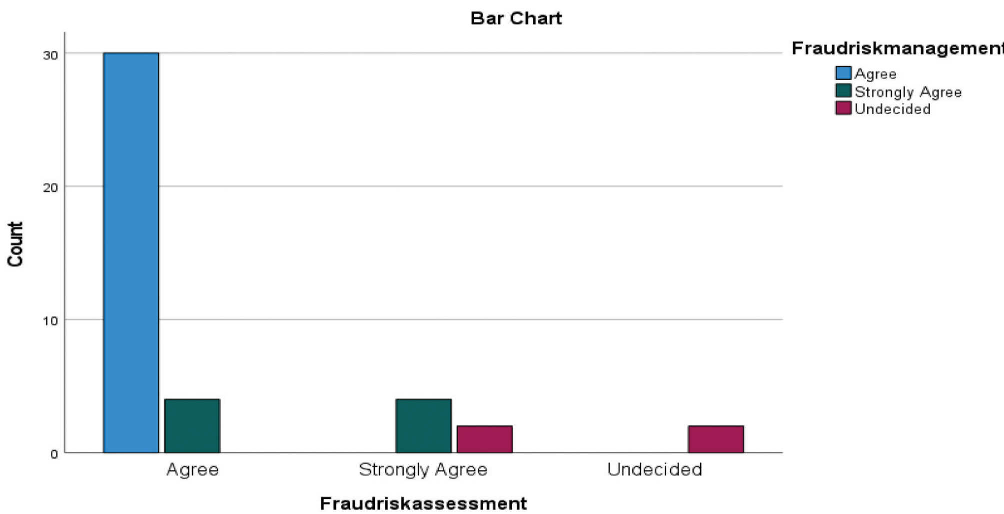
Table 4. Forensic accounting technique implementation for risk assessment and management

Variables	No of response (n) Agree	No of response (n) Strongly Agree	No of response (n) Disagree	No of response (n) Strongly Disagree	No of response (n) Undecided	Total no of respondents (N)
Effective forensic accounting techniques can promote fraud risk assessment	34	6	0	0	2	42
Effective forensic accounting techniques can promote fraud risk management	30	8	0	0	4	42

Source: Field survey

Figure 5. Cross tabulation chart for fraud risk assessment and management with respect to effective forensic accounting application.

Source: Survey results obtained from SPSS



that a positive relationship between the two variables exists. It then means that effective application of forensic accounting can promote both fraud risk assessment and management. The closer the value of the Spearman's correlation coefficient ρ is to 1, the stronger the relationship and the more the interdependence between the two variables and vice versa. Positive values of ρ indicate a positive relationship between the two variables, while negative values of ρ imply a negative relationship (Choi et al., 2010:460).

5. Conclusion and policy implications

Globally, the banking industry has been confronted with various risks, such as fraud risk, interest rate risk, market risk, credit risk, off balance-sheet risk, technology and operational risk, foreign exchange risk, country or sovereign risk, liquidity risk, liquidity risk and insolvency risk. The South African banking industry is well developed in Africa, and it is comparable in sophistication to the financial industries in most developed countries. However, it is not immune against fraud risk. Consequently, fraud risk management demands fraud control. Fraud control is the measure put in place to guide against deviations from normal activities and correct suspected cases of irregularities in the financial statement. Therefore, the purpose of this study was to investigate the application of forensic accounting techniques in relation to fraud risk mitigation. This was achieved using an explanatory research design accompanied with the use of questionnaires involving the purposive sampling method for the 17 licensed commercial banks listed in South Africa. The relationship between the causes of cyberfraud and the influencing factors was established with the aid of the cause-and-effect diagram. The findings substantiate the fact that the loopholes created by non-effective application of forensic techniques are partly responsible for some cyberfraud incidents in the banking industry. However, there is no sufficient evidence to ascertain whether the fraud risk assessment and management in the banking industry has a relationship with the effective application of forensic accounting techniques in terms of the causes of cyberfraud identified in this survey. This calls for the need to establish or introduce some anti-fraud capacities and preventive measures to meet the current demand in information technology and effective moderation of the internal control measures. The implementation of the integration of forensic accounting and management control systems will offer a realistic solution in this regard. However, in terms of the application of forensic accounting for fraud risk assessment and management, the Spearman's non-parametric correlation coefficient carried out gave a positive correlation coefficient that was close to 1 (0.812). This implies that there exists a positive relationship between fraud risk assessment and management and application of forensic accounting. It then means that effective application of forensic accounting can promote both fraud risk assessment and management.

This study is significant in that it has empirical findings that could assist financial institutions in the areas of cyberfraud mitigation as well as decision or policy making. This research notifies the South African banking sector about the possibility of cyberfraud and the way to achieve fraud detection, investigation, prevention, deterrence and risk mitigation via the use of forensic accounting. Since cyberfraud is a digital problem that has assumed a global dimension and since the described situation is not unique to South Africa, other financial institutions in other advanced and emerging economies may also implement the proposed solution based on their peculiarities. This study is limited to the 17 licensed commercial banks registered in South Africa. The analysis is based on the opinions of the bank consultants presenting their own views as well as those of the organisations. Future work can consider the analysis of the measures put in place by the banking industry for fraud risk minimisation.

Funding
The authors received no direct funding for this research.

Author details
Oluwatoyin Esther Akinbowale[1]
E-mail: Oluwatee01@gmail.com
Heinz Eckart Klingelhöfer[1]
Mulatu Fekadu Zerihun[1]
[1] Faculty of Economics and Finance, Tshwane University of Technology (TUT), South Africa.

Disclosure statement
No potential conflict of interest was reported by the author(s).

Citation information
Cite this article as: Application of forensic accounting techniques in the South African banking industry for the purpose of fraud risk mitigation, Oluwatoyin Esther Akinbowale, Heinz Eckart Klingelhöfer & Mulatu Fekadu Zerihun, *Cogent Economics & Finance* (2023), 11: 2153412.

References

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020a). Analysis of cyber-crime effects on the banking industry 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. (2020b). An innovative approach in combating economic crime using forensic accounting techniques. *Journal of Financial Crime*, *27*(4), 253–1271. https://doi.org/10.1108/JFC-04-2020-0053

Albano, P., Castiglione, A., Cattaneo, G., & De Santis, A. 2011. A novel anti-forensics technique for the android OS. *Proceedings of the 2011 International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA)*, pp. 380–385. Maui: IEEE.

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability*, *60*(100989), 1–13. https://doi.org/10.1016/j.jfs.2022.100989

American Institute of Certified Public Accountants (AICPA)., 2012. *Fraud Prevention*. Availableat:www.Aicpa.org/interestareas/forensicandvaluation/resources/fraudpreventiondetectionresponse/, [Accessed: 1st August 2021]

Amigo-Dobaño, L., Garza-Gil, M. D., & Varela-Lafuente, M. M. (2020). Analyzing the attitudes of Spanish firms towards brexit's effects on the management of European fisheries. *Sustainability*, *12*(5819), 1–17. https://doi.org/10.3390/su12145819

Andoh, C., Quaye, D., & Akomea-Frimpong, I. (2018). Impact of fraud on Ghanaian SMEs and coping mechanisms. *Journal of Financial Crime*, *25*(2), 400–418. https://doi.org/10.1108/JFC-05-2017-0050

Apau, R., & Koranteng, F. N. (2019). Impact of cybercrime and trust on the use of e-commerce technologies: An application of the theory of planned behaviour. *International Journal of Cyber Criminology*, *13*(2), 288. https://dx.doi.org/10.5281/zenodo.3697886

Assessment Capacities Projects (ACAPS)., 2012. *Qualitative and quantitative research techniques for humanitarian needs assessment: An introductory brief* https://reliefweb.int/sites/reliefweb.int/files/resources/qualitative_and_quantitative.research_techniques.pdf. [Accessed: 3rd December, 2021]

Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on cell phone forensics. *NIST Special Publication*, *800* (101), 1–75. https://doi.org/10.6028/NIST.SP.800-101r1

Bankscope. 2018. *Bankscope internet quick guide*. https://www.bankscope.bvdep.com [Accessed: 19th October, 2018]

Bassey, B. E., & Ahonkhai, O. E. (2017). Effect of forensic accounting and litigation support on fraud detection of banks in Nigeria. *Journal of Business and Management*, *19*(6), 56–60. https://dx.doi.org/10.9790/487X-1906055660

Boateng, A. A., Boateng, G., & Acquah, H. (2014). A literature review of fraud risk management in micro finance institutions in Ghana. *Research Journal of Finance and Accounting*, *5*(11), 42–52. https://ssrn.com/abstract=2537768

Brockett, P. L., Golden, L. L., & Wolman, W. 2012. *Enterprise cyber risk management. Management for the future - theory and cases*, D. J. Emblemsvåg (Ed.), InTech, Available from: http://www.intechopen.com/books/risk-management-for-the-future-theory-andcases/enterprise-cyber-risk-management [Accessed on 20th June, 2020]. pp. 319–341

Brown, C. S. D. (2015). Investigating and prosecuting cyber crime: forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, *9* (1), 55–119. https://dx.doi.org/10.5281/zenodo.22387

BusinessTech., 2021. *How South Africa's 5 biggest banks continue to dominate*. https://businesstech.co.za/news/banking/506740/how-south-africas-5-biggest-banks-continue-to-dominate/ [Accessed: 13th September, 2021]

Chalil, K. (2000). *Statistical methods for development research* (pp. 1–21). Central University of South Bihar.

Chih-Hao, Y., & Kuen-Chang, L. (2020). Developing a strategy map for forensic accounting with fraud risk management: An integrated balanced scorecard-based decision model. *Evaluation and Program Planning*, *80*1 1–10. https://doi.org/10.1016/j.evalprogplan.2020.101780

Choi, J., Peters, M., & Mueller, R. O. (2010). Correlational analysis of ordinal data: From pearson's r to bayesian polychoric correlation. *Asia Pacific Education Review*, *11*(4), 459–466. https://doi.org/10.1007/s12564-010-9096-y

Clough, J. (2010). *Principles of cybercrime*. Cambridge University Press.

Coetzee, J. (2018). Strategic implications of FinTech on South African retail banks. *South African Journal of Economic and Management Sciences*, *21*(1, a2455), 1–11. https://doi.org/10.4102/sajems.v21i1.2455

Constitution of the republic of South Africa No. 108 of 1996. https://www.gov.za/sites/default/files/images/a108-96.pdf [Accessed: June 29, 2022]

Cusack, B., & Ahokov, T. 2016. Improving forensic software tool performance in detecting fraud for financial statements. In C. Valli (Ed.). *The Proceedings of 14th Australian Digital Forensics Conference*, 5-6 December 2016, Edith Cowan University, Perth, Australia, pp. 17–24.

Dagada, R. 2013. Digital banking security, risk and credibility concerns in South Africa. *The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013)*. Kuala Lumpur, Malaysia, 4 - 6March2013. 978-0-9853483-7-3. The Society of Digital Information and Wireless Communication.

Dellaportas, S. (2013). Conversations with inmate accountants: Motivation, opportunity and the fraud triangle. *Accounting Forum*, *37*(1), 29–39. https://doi.org/10.1016/j.accfor.2012.09.003

Dlamini, S., Mbambo, C., & Ma, W. W. K. (2019). Understanding policing of cybercrime in South Africa: The phenomena, challenges and effective responses. *Cogent Social Sciences*, *5*(1675404), 1–13. https://doi.org/10.1080/23311886.2019.1675404

Dzomira, S. (2015). Cyber-banking fraud risk mitigation conceptual model. *Banks and Bank Systems*, *10*(2), 7–14.

Dzomira, S. (2017). Internet banking fraud alertness in the banking industry: South Africa. *Banks and Bank Systems*, *12*(1), 143–151. https://doi.org/10.21511/bbs.12(1-1).2017.07

Efosa, E. E., & Kingsley, A. O. (2016). Forensic accounting and fraud management: Evidence from Nigeria. *Igbinedion University Journal of Accounting*, *2*(8), 245–308.

Enofe, A. O., Okpako, P. O., & Atube, E. N. (2013). The impact of forensic accounting on fraud detection. *European Journal of Business and Management*, *5*(26), 61–72.

Giudici, P., & Raffinetti, E. (2022). Explainable AI methods in cyber risk management. *Quality Reliability Engineering International*, *38*(3), 1318–1326. https://doi.org/10.1002/qre.2939

Henderson, W. M., & Greaves, P. J. (2011). *Anonymous communications. In A guide to forensic accounting investigation (Second Edition)*. T. W. Golden, S. L. Skalak, M. M. Clayton, & J. S. Pill. PricewaterhouseCoopers. pp. 313–330.

Herselman, M., & Warren, M. (2004). Cyber crime influencing businesses in South Africa. *Issues in Informing Science and Information Technology*, *1*, 253–266. https://doi.org/10.28945/736

Hopkin, P. (2010). *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management* (pp. 1–357). Kogan Page Limited.

Houck, M. M., Kranacher, M.-J., Morris, B., Riley, J. R., Robertson, J., & Well, J. T. (2006). Forensic accounting as an investigative tool. *The CPA Journal*, *76*(8), 68.

Jackson, R. L., II, Drummond, D. K., & Camara, S. (2007). What is qualitative research? *Qualitative Research Reports in Communication*, *8*(1), 21–28. https://doi.org/10.1080/17459430701617879

Kampen, J., & Swyngedouw, M. (2000). The ordinal controversy revisited. *Quality & Quantity*, *34*(1), 87–102. https://doi.org/10.1023/A:1004785723554

Kim, H. Y. (2017). Statistical notes for clinical researchers: Chi-squared test and fisher's exact test. *Open Lecture on Statistics*, https://doi.org/10.5395/rde.2017.42.2.152.152–155.

Kopp, E., Kaffenberger, L., & Wilson, ca.2017. Cyber risk, market failures, and financial stability. *IMF Working Paper No 17/185*. The International Monetary Fund (IMF).

KPMG. 2010. *Fraud and misconduct survey*. Austria and New Zealand pp. 1–48. https://www.aph.gov.au [Accessed on 16th July 2019]

KPMG. 2019. *The multifaceted threat of fraud: are banks up to the challenge? Global banking fraud survey*. www.kpmg.com. [Accessed: 2nd February 2020]

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, *22*(2), 77–81. https://doi.org/10.1080/1097198X.2019.1603527

Leo, M., Sharma, S., & Maddulety, K. (2019). Machine learning in banking risk management: A literature review. *Risks*, *7*(29), 1–21. https://doi.org/10.3390/risks7010029

Lueg, R., & Knapik, M. (2016). Risk management with management control systems: A pragmatic constructivist perspective. *Corporate Ownership and Control*, *13*(3), 72–81. https://doi.org/10.22495/cocv13i3p6

Mishkin, F. S., & Serletis, A. (2011). *The economics of money, banking, and financial markets* (4th edn) ed.). Pearson Canada Inc.

Modugu, K. P., & Anyaduba, J. O. (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.

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/10.1016/j.sbspro.2016.05.499

Moyo, B. (2018). An analysis of competition, efficiency and soundness in the South African banking sector. *South African Journal of Economic and Management Sciences*, *21*(1), 1–14. https://doi.org/10.4102/sajems.v21i1.229

Nissan, E. (2012). The forensic disciplines: some areas of actual or potential application [Nissan 2012. In *Computer applications for handling legal evidence, police investigation and case argumentation* Vol. 5(1) (pp. 841–989). Springer. https://doi.org/10.1007/978-90-481-8990-8

Okoye, E. I., & Gbegi, D. O. (2013). Forensic accounting: A tool for fraud detection and prevention in the public service. (A study of selected ministries in Kogi State). *International Journal of Academic Research in Business and Social Sciences*, *3*(3), 1–18.

Omar, N. B., Mohamed, N., & Jomitin, B. 2013. The relevance of forensic accounting in public sector (A study of selected government agencies in Klang Valley). *The 5th International Conference on Financial Criminology (ICFC), Malaysia. "Global Trends in Financial Crimes in the New Economies"* pp. 225–232.

Oppenheim, A. N. (1992). *Questionnaire design, interviewing and attitude measurement*. Pinter.

Ospina, S. (2004). Qualitative Research. In G. Goethals, G. Sorenson, & J. MacGregor (Eds.), *Encyclopedia of Leadership* (pp. 1279–1284). London: SAGE.

Peshori, K. S. (2015). Forensic accounting a multidimensional approach to investigating frauds and scams. *International Journal of Multidisciplinary Approach and Studies*, *2*(3), 26–35.
Radanliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., & Burnap, P. (2018). Future developments in cyber risk assessment for the internet of things. *Computers in Industry*, *102*, 14–22. https://doi.org/10.1016/j.compind.2018.08.002
Report, P. 2019. *The Future of Banking: A South African Perspective*. www.pwc.ac.za. [Accessed on 20th June 2020]
Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence*, *2* (3, vol), 1–28.
Ruan, K. (2017). Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Computer & Security*, *65*, 77–89. https://doi.org/10.1016/j.cose.2016.10.009
Saddiq, S. A., & Bakar, A. S. A. (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. https://doi.org/10.1108/JFC-10-2018-0112
Santos Filho, C. R., Carlos, F. A., & Costa, F. M. (2017). Relevant skills for criminal accounting expertise: The perception of federal police experts and delegates. *Journal of Education and Research in Accounting*, *11*(1), 69–88. https://dx.doi.org/10.17524/repec.v11i1.1446
Saunders, A., & Cornett, M. M. (2017). *Financial institutions management: A risk management approach* (9th edn) ed.). McGraw Hill.
Shah, S., Weintraub, D., & Miller, F. R. (2011). Foreign corrupt practices act. In T. W. Golden, S. L. Skalak, M. M. Clayton, & J. S. Pill (Eds.), *A guide to forensic accounting investigation, second edition* (pp. 527–546). PricewaterhouseCoopers.
Shin, J., Son, H., Heo, G., & Heo, G. (2015). Development of a cyber security risk model using Bayesian networks. *Reliability Engineering and System Safety*, *134*, 208–217. https://doi.org/10.1016/j.ress.2014.10.006
Smith, G. S., & Crumbley, D. L. (2009). Defining a forensic audit. *Journal of Digital Forensics, Security and Law*, 4 (1), 61–80. https://doi.org/10.15394/jdfsl.2009.1054
South African Banking Report. 2019. https://www.globenewswire.com/news-release/2019/02/20/1738270/0/en/South-Africa-Banking-Industry-Report-2018.html. [Accessed 1st June, 2019].
South African Reserve Bank (SARB). 2020. *Management of the South African money and banking system* https://www.resbank.co.za/AboutUs/Functions/Pages/Management-of-the-South-African-money-and-banking-system.aspx. [Accessed: 2nd February, 2020]
Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *National Institute of Standards and Technology Special Publication*, *800*(30), 1–53.
Sutherland, E. (2017). Governance of cybersecurity – the case of South Africa. *The African Journal of Information and Communication*, *20*, 83–112. https://dx.doi.org/10.23962/10539/23574
Ugoni, A., & Walker, B. F. (1995). The chi-square test: An introduction. *Comsig Review 62*, 4(3), 61–64. https://pubmed.ncbi.nlm.nih.gov/17989754/
von Solms, S., Louwrens, C. P., Reekie, C., & Grobler, T. (2006). A control framework for digital forensics. In O. M. & S. Shenoi (Eds.), *International Federation for Information Processing, Voltulle 222, Advances in Digital Forensics II* (pp. 343–355). Boston: Springer.
Wanemba, M. A. (2010). *Strategies applied by commercial banks in Kenya to combat fraud. A management research project submitted in partial fulfilment of the requirements for the award of the degree of master of business administration*. Department of Business Administration, School of Business, University of Nairobi.
Wells, J. T. (2003). The fraud examiners. *Journal of Accountancy*, *196*(4), 76.
Wilson, T. P. (1977). Critique of ordinal variables. *Social Forces*, *49*(3), 432–444. https://doi.org/10.2307/3005735
Wilson, N., & Mcclean, S. (1994). *Questionnaire design: A practical introduction. University of Ulster. Copies available from: UCoSDA, Level Six* (pp. S10 2TN). University House, University of Sheffield.
Wright, R. E. (2011). *Finance, banking and money. Sioux falls, S.D* (pp. 1–525).
Zakaria, K. M., Nawawi, A., & Salin, A. S. A. (2016). Internal controls and fraud – empirical evidence from oil and gas company. *Journal of Financial Crime*, *23*(4), 1154–1168. https://doi.org/10.1108/JFC-04-2016-0021