




Exploring the level of information security in the South African banking industry

 **Oluwatoyin Esther Akinbowale**^{1*}

 **Heinz Eckart Klingelhofer**²

 **Mulatu Fekadu Zerihun**³

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

¹Email: oluwate01@gmail.com

²Email: KlingelhoferHE@tut.ac.za

³Email: ZerihunMF@tut.ac.za



(+ Corresponding author)

ABSTRACT

Article History

Received: 23 June 2023

Revised: 6 October 2023

Accepted: 19 December 2023

Published: 9 January 2024

Keywords

Anti-fraud technologies

Banking industry

Cyberattack

Information security.

The purpose of this study is to explore the level of information security among South African banks with the aim of determining the level of their resilience to cyberattacks and intrusions. The study employs a mixed approach that involves both quantitative and qualitative analyses of the responses obtained from a structured questionnaire used as the survey instrument. The questionnaire was distributed to some selected members of staff of the 17 licensed banks in South Africa saddled with the responsibilities of operation, customer service, management, and administration. In addition, non-parametric statistical analyses such as Fischer's Exact and Chi-square tests, as well as Spearman's correlation, were carried out. The outcome of this study indicated that the effectiveness of information security on customers' service in the South African banking industry is assumed to be high. South African banks are deploying different anti-fraud technologies to strengthen the level of information security; however, there are still substantial cases of cyberfraud and unauthorised intrusions. The findings also indicate that the integration of forensic accounting and management control systems may promote information security in the banking industry. This study provided an insight into the impact of information security framework development to reduce systems' vulnerability and intrusions.

Contribution/Originality: The novelty of this work includes an analysis of the level of information security in the South African banking industry and the development of an information security framework that has not been widely reported in the existing literature.

1. INTRODUCTION

Nowadays, the operations of many financial institutions are digital and automated, with the merits of effective delivery, speed, and ease of operation. However, these merits come with some potential vulnerabilities, such as information security challenges and cyber-insecurity, among others (Ali, Ali, Surendran, & Thomas, 2017). In recent years, information and cyber insecurity have been major challenges that organisations have to deal with (Network Encyclopedia, 2023). The increasing evolution of digital technologies, as well as banking innovations and applications that allow remote access to banking services, have increased the risk of cyber insecurity and data breaches. This is coupled with the fact that the global pandemic era redefined the way in which businesses are operated. Business operations are becoming increasingly flexible to accommodate remote participation. This has given rise to more digital banking applications, the Internet and mobile banking services, but with significant

threats to critical banking infrastructures, as threat actors often exploit the vulnerabilities of these digital systems to commit fraud from any location. Furthermore, [Gebremeskel, Jonathan, and Yalew \(2023\)](#) stated that the over-reliance of business organisations on Information Technology (IT) and big data for value creation, products and services improvement have made information a valuable asset to both the organisation and the threat actors. Thus, information and cyber security are some of the major issues faced by the banking industry today. The threat landscape is increasingly evolving with the evolution of digital technologies, and some of the critical banking infrastructures are not designed to be resilient to these attacks. Information and cyber security breaches have direct consequences on the organisation's profitability, reputation, and good will, as well as customers' satisfaction ([Network Encyclopedia, 2023](#)). For any organisation to fully explore and harness the potential and benefits of digital transformation, information and cyber-security challenges must be dealt with appropriately ([Gebremeskel et al., 2023](#)). Hence, organisations must take proactive steps to ensure data protection from cyberattacks through the implementation of cyber-security measures.

1.1. Overview of Information Security

Information security involves the act of preventing intrusions in the form of unauthorised access, use, disruption, recording, disclosure, modification, distribution, inspection, or destruction of the organisation's and customers' information stored in digital and non-digital forms ([Sattarova Feruza & Kim, 2007](#); [Tiwari, Bhalla, & Rawat, 2016](#)). While cybersecurity deals with the protection of information stored in digital systems within the cyberspace, information security encompasses the protection of personal or organisational data stored both within the digital and non-digital systems and within and beyond the cyberspace. Thus, information security is a broad division of technology that is applicable to networks for data or information protection and the protection of an organisation's assets from theft, natural disaster, and misuse ([Agarwal, Gupta, Gupta, & Gupta, 2011](#); [Jhavar & Piuri, 2017](#)). Information security also ensures that the protected information is made available to only authorised users ([Agarwal et al., 2011](#); [Jhavar & Piuri, 2017](#)). [Tiwari et al. \(2016\)](#) define information security as the integration of procedures and technologies intended to safeguard networks and information from intrusions by cybercriminals.

Information security means the protection of data or information systems effectively from unauthorised intrusion ([Sattarova Feruza & Kim, 2007](#)). Information and cybersecurity, as well as the integrity of data, are some of the prominent challenges in the banking industry today, despite regulatory and organisation's efforts in terms of controls and measures to prevent intrusions and cyberfraud. The ultimate purpose of information security measures is to protect the organisation's system and the various data and safeguard the customers' information from intrusion and theft in order to promote a safe and effective operation ([Sattarova Feruza & Kim, 2007](#)). [Holappa et al. \(2005\)](#) explain that information security involves the sum of technical and administrative activities deployed to ensure information safety and also guarantees data access to only authorised users without any form of intrusion from unauthorised persons.

1.2. Cyberfraud and Information Security Management

With the pace of digital transformation, there is a need for business organisations to secure their information management systems to avert their vulnerability to cyberattacks. The implementation of a robust information security system can prevent unauthorised intrusions into the organisation's system and database and also provide a proactive means of responding to threats emanating from cyberattacks. In addition to this, there is a need to keep the staff abreast of the emerging technologies through sensitization, training, and initiatives aimed at increasing staff awareness about information security issues. The organisation's management also needs to formulate and implement effective policies to promote information security and update them periodically to ensure they meet acceptable standards and meet the dynamic security challenges ([Carenys, 2012](#); [Mohammeda & Knapkova, 2016](#); [Slavoljub, Srdjan, & Predrag, 2015](#)). To mention a few: first, sources of threats and vulnerabilities, including their

risk levels, must be identified and evaluated. Second, there is a need to establish and implement effective control measures and procedures to mitigate the identified risk and measure the performance of the controls employed. Having established the fact that a well-implemented information security management system can promote an organisation's resilience to cyberattacks, it is worth mentioning that the relevant framework as well as supporting technical capabilities and technologies must be put in place.

Information security breaches in South Africa have been linked to poor maintenance culture of the financial institutions, failure to perform periodic checks and inadequate audits of security and incident logs, poorly implemented security strategies, including application software, poor control and monitoring of cyber systems, weak incident response capabilities, inadequate security assessment and sensitisation, as well as poor or lack of policy and standard management (Mbeli & Dwolatzky, 2016). In South Africa, Sutherland (2017) observed that poor service delivery has resulted in inadequate risk assessments, a lack of transparency, and improperly coordinated efforts across business, government, and society. In order to avert huge losses owing to cybercrime, the use of a real-time alert system that can bring potential fraudulent activities to the notice of both customers and financial institutions has been suggested (Akinbowale, Klingelhöfer, & Zerihun, 2020a). Akinbowale, Klingelhöfer, and Zerihun (2020b) also proposed two streamlined conceptual models for cyberfraud mitigation. The first one integrates the concept of forensic accounting into the organization's control structure, while the second model presents an in-depth investigation and an all-inclusive data analysis framework for fraud detection.

1.3. Forensic Accounting and Management Control Systems for Cyberfraud Mitigation

There is a consensus that the deployment of forensic accounting techniques is an appropriate method that can sufficiently promote fraud mitigation and information security (Alabdullahi, Alfadhi, Yahya, & Rabi, 2013; Chi-Chi & Ebimobewe, 2012; Cusack & Ahokov, 2016; Okoye & Akamobi, 2009; Perduv, Ceklic, & Ceklic, 2018; Serhii, Vadym, Oleg, Oleksandr, & Strilets, 2019; Wells, 2003). There is also a convergent view on the fact that a good management control system has the capability to enhance the performance of an organisation. The organisation's performance is inclusive of information and cyber security as well as fraud mitigation (Carenys, 2012; Henri & Journeault, 2010; Mohammeda & Knapkova, 2016; Slavoljub et al., 2015; Tekavčić & Peljhan, 2003). Since existing studies have indicated the feasibility of applying either forensic accounting or management control systems for fraud mitigation and to achieve information security, this study investigates the level of information security in the South African banks via a survey and further explores the possibility of combining forensic accounting and management control systems to promote information security. In view of this, the three alternative hypotheses underlying this study are formulated as follows:

H₁: The level of information security in the South African banking industry is high.

H₂: The level of effectiveness of information security on customers' service in the South African banking industry is high.

H₃: The integration of forensic accounting and management control systems can promote information security in the South African banking industry.

This study is based on the space transition theory with the purpose of exploring the level of information security in the South African banking industry to determine the level of resilience to cyberattacks and unauthorised intrusions. The objectives of this study include the gathering of primary data relating to information security through a survey using a structured questionnaire as the survey instrument and the statistical analysis of the data gathered. Hypothesis formulated are also tested, and conclusions are drawn from the results obtained. This study gives an understanding of the importance of information security to reduce the system's vulnerability to unauthorised intrusions. Therefore, the results of this study could help financial organisations create an integrated information security system that can withstand cyberattacks. The novelty of this work includes an analysis of the level of an information security in the South African banking industry and the development of information security framework that have not been widely reported in the existing literature.

The succeeding sections present the methodology employed in this study, the results and discussion, the conclusion obtained from the findings of the study vis-à-vis the study's objectives, and end with the policy recommendations.

2. LITERATURE REVIEW

This study falls under the auspice of the *space transition theory* that deals with crimes of the internet and explains that the nature and behaviour of persons determine whether their conducts will be compliant with the societal and cyberspace requirements (Jaishankar, 2008). The growing number of internet users, coupled with data evolution and the use of emerging technologies, has progressively exposed individual's and organisation's information to several risks. Cyberfraud is becoming more common in this digital era (Akinbowale et al., 2020b; Ali et al., 2017; Rao, 2019; Tiwari et al., 2016; United Nations Office on Drug Crime, 2013). Hence, the development, upgrading, and implementation of a robust information security system are essential for any financial institution to mitigate the challenge of cyberfraud. Such attacks could be in the form of intrusions into personal accounts or an organisation's database with the aim of manipulating or hijacking business operations to commit fraud (Tiwari et al., 2016). In addition, it could take the form of information or data breach where confidential data is manipulated or stolen. Existing studies have indicated that cyberfraud impacts financial organisations negatively in the form of loss of revenue and profitability, decline in the level of customers' satisfaction, loss of reputation and good will, as well as information security and risk management (Goel & Shawky, 2009; Kraemer-Mbula, Tang, & Rush, 2013; Lagazio, Sherif, & Cushman, 2014; Martin & Rice, 2011; Saini, Rao, & Panda, 2012; Skalak, Alas, & Sellito, 2011).

In addition, effective information security and operations management are part of the major success factors that can help any organisation achieve the goals of cyberfraud mitigation (Choobineh, Dhillon, Grimaila, & Rees, 2007). According to Choobineh et al. (2007), information security management faces three main challenges:

- First, information security is generally perceived as an afterthought. This implies that some financial institutions do not usually invest in proactive and preventive information security measures until after the occurrence of an attack.
- Second, since information security is perceived as an afterthought, the response of some financial institutions to cybercrime may be more reactive than proactive.
- Third, basically, some conceptualised frameworks aimed at promoting information security remain theoretical in nature. This implies that there is poor implementation of conceptual frameworks for information security.

According to Usher (2006), information security encompasses five essential terms: integrity, confidentiality, application security, network security, and host security (Usher, 2006).

Kadiri (2014) and Khan and Barua (2009) have raised concerns about the challenges of information security in the banking sector because of emerging technologies. Mbeli and Dwolatzky (2016) also stated that information security, including data breaches and system compromises, are prominent challenges in the financial sector. Although, in some financial institutions there are in general strong control practices to prevent unauthorised access, new ways of data theft and fraud perpetration are constantly emerging (Mbeli & Dwolatzky, 2016). Ali et al. (2017) identified the lack of proper management of information security risk as a major contributing factor to the increase in the rate of cyberfraud. Lee and Lee (2012) found that information security challenges can stimulate the negative responsive behaviours of customers against compromised service providers. This may affect the reputation of such a financial institution and impact the confidence of the customers in the services provided. Akelola (2012) indicated that the management control systems of some financial institutions are not robust enough due to a lack of funds for sustaining Information Technology (IT) facilities that aid information security.

Malik and Islam (2019) posited that effective sensitisation, education, and awareness about information and cybersecurity are crucial to cyberfraud mitigation. Therefore, the banking industry should raise awareness and educate the public on how to avoid unauthorised access to their accounts. In the opinion of Rowlingson (2004),

information security programmes are often employed as preventive and detective measures against fraud occurrences. In South Africa, Mbeli and Dwolatzky (2016) explain that information and cyber security challenges are major threats to economic wellbeing of the financial institutions and the country. This prompted the banking sector to incorporate risk management processes as an integral component of their business plan. Therefore, the authors suggested continuous investment in up-to-date technologies and security measures as a proactive way to salvage the situation. Van Niekerk (2017) found the hackers top the list of threat actors in South Africa. Data breaches and cash theft top the list of impacts due to cyberfraud. Gebremeskel et al. (2023) identified some of the information security issues faced by some organisations that embraced the digital transformation of business processes. These include: financial challenges, the risk of information and security breaches, and a lack of the required expertise to implement information security measures, among others. Maglaras et al. (2020) provided some policy recommendations for tackling information and cyber-insecurity. These include the formulation and implementation of new policies relating to data protection, e-communications, and the security of products and services, as well as the proper coordination and mapping of the procedures and requirements for information and cyber-security at the technical and organisational levels. In addition to these stated measures, as part of the risk management approach, incident notification and response strategies that can assist in preventing cyberattack and managing cybersecurity incidences effectively must be deployed. Georgili and Pitsi (2022) stated that achieving information security is one of the major conditions that can instill customers' confidence. The authors identified several policies that can be implemented to promote information security. These include: configuration security, execution and access control, user authentication, network and malware protection, event log registries, teleworking and cryptography, education, training, and awareness of supply chain risk management; cybersecurity technical assessment; data backup; incidence and disaster handling, recovery and business continuity policies, among others.

3. DATA AND METHODOLOGY

This study uses data collected from the 17 South African licensed banks (Bank scope database). Figure 1 presents the research design developed for this study. The mixed approach involves both quantitative and qualitative analyses of the responses obtained from a questionnaire used as a survey instrument for data collection. The questionnaire was distributed to some selected members of staff of the banks in South Africa saddled with the responsibilities of operation, customer service, management, and administration, as well as decision-makers and those who are directly involved in fraud mitigation. The essence is to garner reliable and detailed information on the organisation's ongoing and expended efforts on cyberfraud mitigation. In addition, non-parametric statistical analyses such as Fischer's Exact and Chi-square tests, as well as Spearman's correlation, were conducted. The data garnered from the questionnaires was analysed to ensure an assenting outcome void of bias. The reason for using questionnaires was due to their capabilities to capture, quantify, and verify complex matters like cyberfraud. It also permits the quick gathering of responses in a consistent way (Oppenheim, 1992; Wilson & Mcclean, 1994). Questionnaire items were formulated based on the aim of this study using a variety of questions ranked in order of their importance.

Existing studies such as Ko and Dorantes (2006); Kong, Jung, Lee, and Yeon (2015); Ali et al. (2017) and Dzumira (2017), have relied only on survey and empirical approaches to examine the impact of cyber-attacks and information security breaches on organisation's performance and customers' satisfaction. In addition to the survey carried out in this study, an integrated information security framework was also developed to promote information security in the banking industry.

The collected data were qualitative in nature and comprised nominal data types ("yes" and "no") and ordinal data types (Likert-type response format). The collected data were thereafter coded for easy handling and analysis.

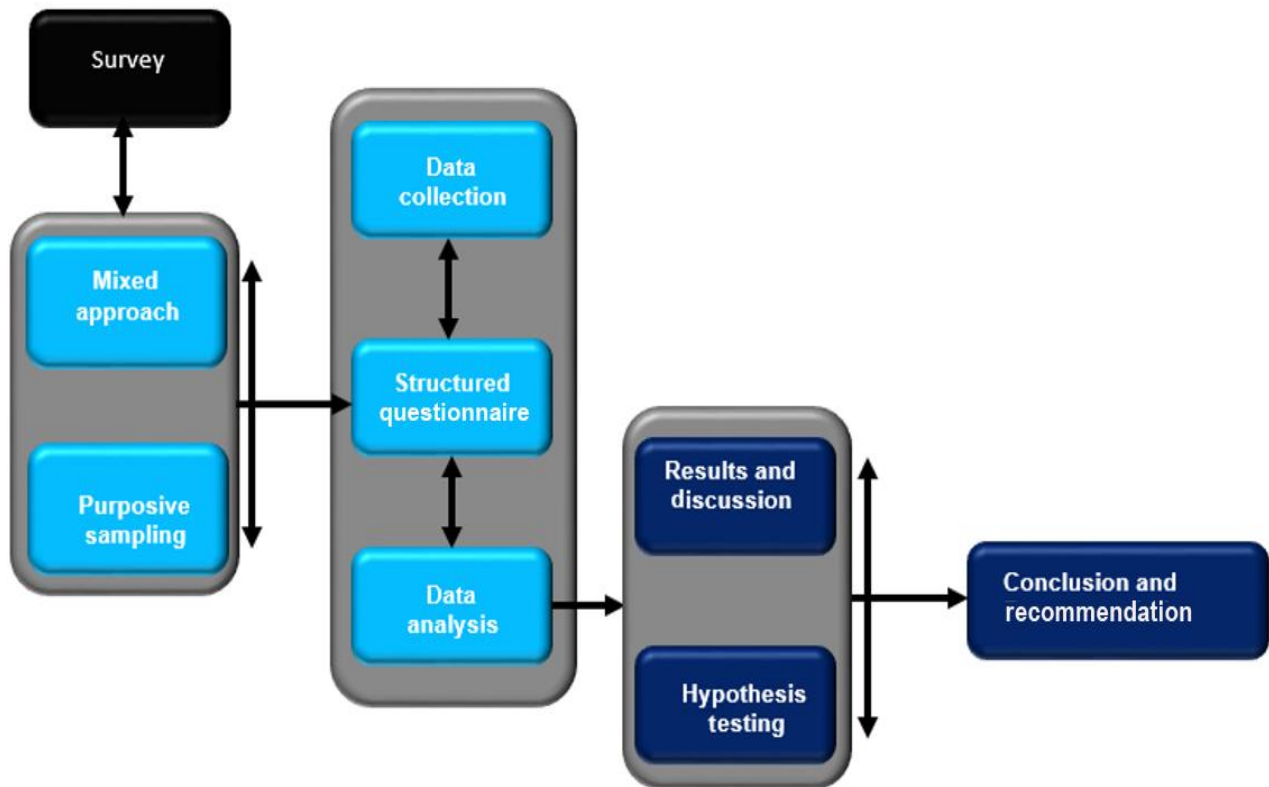


Figure 1. Research design.

To test the three hypotheses mentioned under 1.3, non-parametric statistical analyses as well as inferential statistics were conducted with the aid of the Statistical Package for Social Science (SPSS) version 26. The non-parametric analysis includes the cross tabulation, Fischer's Exact and Chi-square tests, and Spearman's correlation. The inferential statistics were employed for testing the hypothesis developed using the chi-square(χ^2) statistics, while the Fischer's Exact test statistics were employed to ascertain the association between some variables to determine whether two factors in the same group are dependent or independent on each other. The collected data were coded to allow for qualitative analysis to be performed and to simplify the data analysis process to obtain a reliable outcome.

4. RESULTS AND DISCUSSION

H: The level of information security in the South African banking industry is high.

This hypothesis was tested using the responses obtained from the question on the "effect of information security on an organisation's profitability." The alternative hypothesis tested was therefore accepted because the p-value was 0.001. The fact that the p-value was less than 0.05 indicates that there is insufficient evidence to accept the null hypothesis at the 5% significance level. Thus, this led to the acceptance of the alternative hypothesis, and the statement "information security level in the South African banks is high" is assumed to be true with the presented evidence.

Table 1 illustrates the impact of information security on an organisation's profitability. This result indicates that information security has a large effect on the profitability of the banking industry. This is because information is key to the banking industry, as the trend of operations can only be effectively monitored through available information.

The Pareto chart employed in Figure 2 shows the magnitude of the impact of information security on organisational profitability. Information security refers to the process of ensuring that sensitive information about the organisation is properly protected from both internal and external intrusions. The left vertical axis of the bars

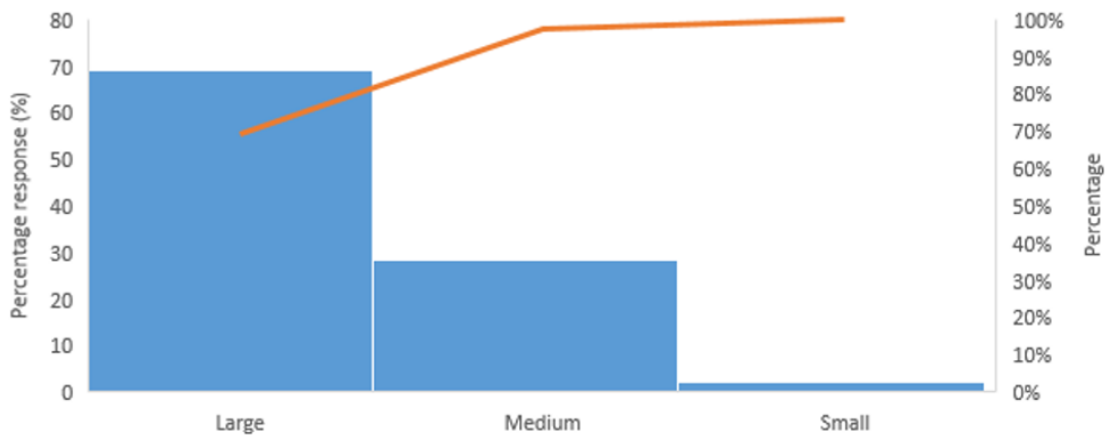
represents the percent contribution of information security to organisational profitability, while the right vertical axis is the percent demarcation. The plot shows that information security plays a significant role in the organisation’s profitability. Moreover, the cumulative line’s steepness suggests that information security has a significant impact on the organization’s profitability. The large difference in the percentage demarcation at the right vertical axis of the Pareto chart further lends credence to the fact that the effect of information security on organisational profitability is indeed quite significant.

In line with some of the existing literature, the importance of this finding is that there exists a direct relationship between information security and organisational profitability. For instance, the proposals of Dzumira (2017) and Van Niekerk (2017) emphasise the need to strengthen information security and increase sensitisation of internet users to the nature of internet banking fraud perpetrated by cybercriminals in South Africa. Also, Obeng-Adjei (2017) indicates the South African banking industry needs to implement stringent security controls across their networks and other supporting infrastructure, such as databases and servers, to protect customers’ information. The study further recommends the implementation and enforcement of access controls to tighten information security.

Ko and Dorantes (2006) found indications that security breaches are detrimental to organisational profitability. Hence, information security can reduce the negative impact of cyberfraud on organisational performance, as banks with high levels of information security will be able to lessen the occurrences of cyberfraud (Finau, Samuwai, & Prasad, 2013; Malik & Islam, 2019).

Table 1. Effect of information security on organisation’s profitability.

Effect of information security on organisational profitability	Number of response (n)	Percentage response (%)
Large	29	69.04
Medium	12	28.57
Small	1	2.38
Total	42	100



H₂: The level of effectiveness of information security on customers’ service in the South African banking industry is high

This hypothesis was tested based on the responses obtained from the “level of information security risk and information security effectiveness on customers’ service.” Table 2 presents the Chi-square and the Fischer’s Exact tests for the level of information security risk.

Table 2. Chi-square and Fischer’s exact tests for the level of information security risk.

IT based services	Chi-square statistics	Degree of freedom (Df)	Asymptotic significance (Asymp. sig.)	Fischer’s exact significance	Point probability
Level of information security risk	17.714	2	0.000	0.000	0.000
Level of effectiveness of information security risk on customers’ service	14.714	2	0.001	0.001	0.001

The tested alternative hypothesis was accepted because the p-values of the factors (IT-based services, specifically the information security risk level and the level of effectiveness of information security risk on customers’ service) were 0.000 and 0.001 (significantly less than 0.05 for both factors). This implies that, with the evidence presented in this study, the level of effectiveness of information security on customers’ service in the South African banking industry is assumed to be high.

Tables 3 and 4, respectively, indicate the level of information security risk and the impact on customer services in the South African Banking industry. These findings show that the information security risk in the banking industry has a huge effect on customers because they are the bearers of most of the sensitive information available in the industry. The effect of information security risk was further depicted using a bar chart Figure 3 which shows that information security risk is a threat to the banking industry and that information security enhances customers’ services.

Table 3. Information security risk.

Information security risk	Number of responses “Very high”	Number of responses “High”	Number of responses “Low”	Total number of respondents
Level of information security risk (LISR)	24	16	2	42
Level of effectiveness of information security risk on customers’ service (LEISRCS)	23	16	3	42

Table 4. Information security risk (%).

Information security risk	Percentage response (%) (Very high)	Percentage response (%) (High)	Percentage response (%) (Low)	Total percent response (%)
Level of information security risk	57.14	38.09	4.76	100
Level of effectiveness of information security on customers’ service	54.76	38.09	7.14	100

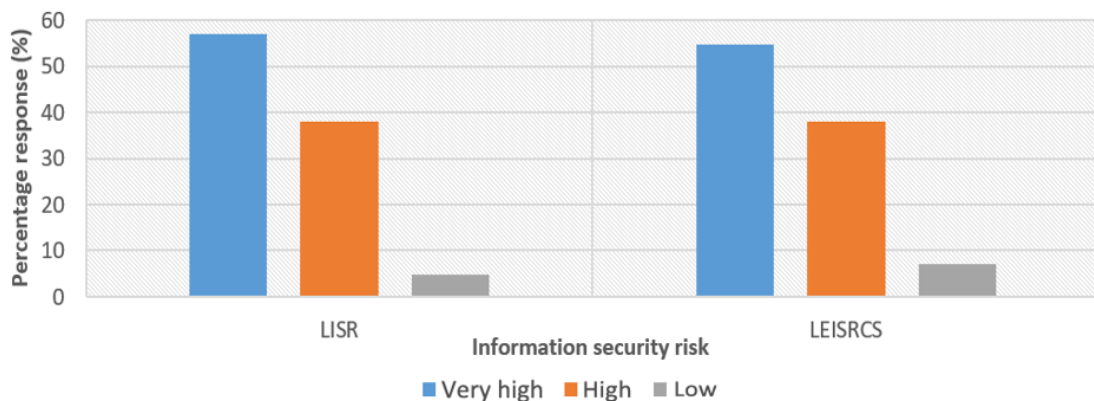


Figure 3. Level of information security risk (LISR) and information security effectiveness (LEISRCS) on customers’ service.

These findings refute the results of Dagada (2013), who claimed that the operation of digital banking (specifically mobile and online banking) was not affected adversely by security lapses. The author reported that bank customers in South Africa embraced digital banking services instead of cash transactions and that the aggressive way with which South African banks were tackling cybercrime had shielded their customers from the impact of cybercrime (Dagada, 2013). On the global level, some existing literature has also submitted that effectively managed information security can reduce the impact of cybercrimes and enhance organisational performance significantly (Kong et al., 2015; Koo, Park, & Park, 2013; Malik & Islam, 2019).

The cross-tabulation of the two factors of IT-based services, “level of information security risk” and “information security effectiveness on customers’ service”, gave a Fischer’s Exact statistical value of 3.554 and a p-value greater than 0.05 (0.494 > 0.05) at four degrees of freedom and a 95% significance level. This implies that there is insufficient evidence to substantiate the assumption that the relationship existing between the two above-mentioned factors is interdependent (see Table 5).

Table 5. The statistical analysis for the pair of the level of information risk and the effectiveness on customers’ service.

Paired factors	Fischer’s exact test statistics	Degree of freedom (df)	Exact sig. (2 tailed)	Remarks	Spearman’s correlation coefficient	Relationship
Level of information risk and the effectiveness on customers’ service	3.554	4	0.494	5 cell (55.6%) have expected outcomes less than 5. The minimum expected count is 0.14	-0.181	Negative and weak

Spearman’s non-parametric correlation was conducted to establish the type of correlation existing between the two factors. The result gave a correlation coefficient of -0.181. This suggests that a quite small negative relationship seems to exist between the two variables. Hence, when the level of information security risk increases, there will be a slight reduction in the effectiveness of customers’ satisfaction, and vice versa.

H₃: The integration of forensic accounting and management control systems has the ability to promote information security in the banking industry.

This hypothesis was tested based on the responses obtained from the effect of cyberfraud on customers’ satisfaction and IT-based services.

Table 6 presents the results of the Chi-square and Fischer’s Exact statistics conducted to investigate the impact of cyberfraud occurrences on customers’ satisfaction. The p-values obtained for both tests are 0.000 (0.000 < 0.05). This led to the acceptance of the alternative hypothesis suggesting that the integration of forensic accounting and the management control systems may promote information security in the banking industry. Therefore, the integration of forensic accounting and the management control systems may be a viable method for cyberfraud mitigation.

Table 6. Chi-square and Fischer’s exact tests for the effect of Cyberfraud on customers’ satisfaction.

Statistical parameter	Value
Chi-square statistics	16.714
Df	2
Asymp. sig.	0.000
Fischers’ exact sig.	0.000
Point probability	0.000

As a result of this, even the level of the organisation’s profitability and customers’ satisfaction may be enhanced, as already reported by Peikari (2010) and Lee and Lee (2012). In other words, when the level of information security is low, the rate of cyberfraud is likely to increase with an increase in customers’ dissatisfaction, and vice versa. This also lends credence to the already established fact that the integration of forensic accounting and management control systems has the tendency to combat cyberfraud, thereby ensuring customer satisfaction through an improved information security system.

The responses obtained from the customers’ experience about the effect of cyberfraud on three customer satisfaction levels over the years are presented in Table 7.

Table 7. Effect of Cyberfraud.

Effect of cyberfraud	Number of response (n)	Percent response (%)
Highly consequential (HC)	23	54.76
Consequential (C)	17	40.47
Trivial (T)	2	4.76
Total	42	100

The results imply that in most cases, the effect of cyberfraud on customers in the banking industry cannot be downplayed or taken with negligence, as this can cause customers to lose confidence in the bank’s digital services. This outcome agrees with the findings of Du Toit, Hadebe, and Mphatheni (2018), who reported that a significant number of South Africans have fallen victim to cybercrime in recent years and see the effect of cybercrime on customers as critical.

Also, other studies have categorised the impact of cyberfraud on customers’ satisfaction as highly consequential (Böhme & Moore, 2012; Lagazio et al., 2014; Saini et al., 2012). A bar chart was employed to show the magnitude of the effect on the customers’ satisfaction level to determine the severity of the effect of cyberfraud Figure 4.

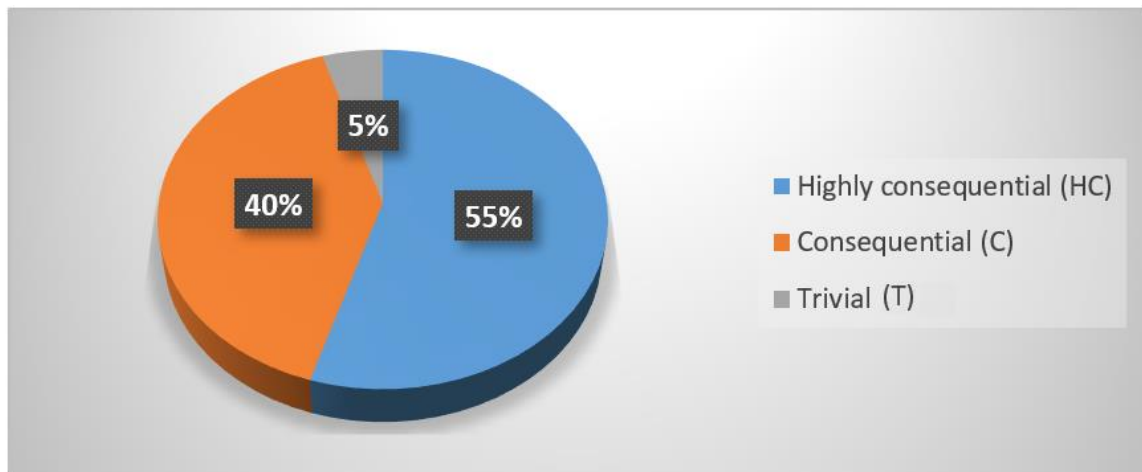


Figure 4. The effect of Cyberfraud on customers’ satisfaction.

With the aid of the bar chart, the severity of the consequences of the effect of cyberfraud experience on the customer satisfaction level in the South African banking industry over the years was easily distinguished. This will assist in raising awareness of cyberfraud as one of the factors that contributes significantly to customers’ dissatisfaction.

Table 8 presents the Chi-square and the Fischer’s Exact test for the IT-based services. The nature of IT-based services employed by the organisation has been linked to the level of information security (Shrivastava, 2016).

Table 8. Chi-square and Fischer’s tests for the IT based services.

IT based services	Chi-square statistics	df	Asymp. sig.	Fischer’s exact sig.	Point probability
Tele banking	52.000	2	0.000	0.000	0.000
Merchant service	43.000	2	0.000	0.000	0.000

Since information security deals with the frameworks, guidelines, and technical solutions employed to safeguard personal and organizational information to prevent intrusion and damage to information systems and other IT-based services (Shrivastava, 2016), seven variables were employed for testing this hypothesis: credit banking, electronic fund transfer, online banking, electronic debit, and internet banking, telebanking and merchant services. Following the hypothesis testing, the alternative hypothesis tested was therefore accepted for two variables (telebanking and merchant services) because the p-values for each of these variables stand at $0.000 < 0.05$ for both tests. This implies that the integration of forensic accounting and the management control system may promote information security in the banking industry, provided the IT services are effectively implemented and controlled. For the other five types of variables (credit banking, electronic fund transfer, online banking, electronic debit, and internet banking), the Chi-square could not be performed because there were no differences in the answers; all the respondents unanimously confirmed that these IT-based services were employed in their banks.

Table 9 shows the percentage responses obtained for the nature of the IT-based services available in the South African Banking industry; the percentage frequencies of the available IT-based services are depicted in Figure 5. From Table 9, there was 100% agreement by the respondents who opined that their banks use IT-based services such as credit banking, electronic fund transfers, online banking, electronic debit cards, and internet banking, except for telebanking and merchant services, where few respondents were undecided. The results obtained imply that most of the banks have integrated IT-based facilities into their services.

Table 9. Suggested IT based services.

Suggested IT based services	Percentage response (%) (Yes)	Percentage response (%) (No)	Percentage response (%) (Don’t know)	Total percent response (%)
Credit card service	100	0	0	100
Tele banking	88.09	4.76	7.14	100
Electronic fund transfer	100	0	0	100
Online corporate banking	100	0	0	100
Electronic debit card	100	0	0	100
Merchant account services	83.33	4.76	11.90	100
Internet banking	100	0	0	100
Others (Card less)	23.80	0	0	23.8

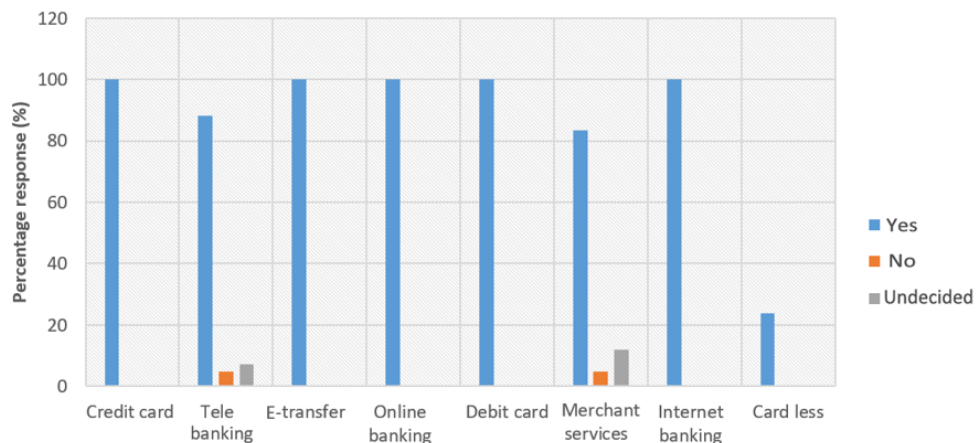


Figure 5. The IT based services available in the South African banking industry.

This finding is in line with the report of the Centre for Excellence in Financial Service (2017), which indicates that in South Africa, the emergence of digital technology has continued to change the structure of the financial market and transform business operations. The report explains that the infusion of technology into the financial sector has improved the customers' experience with fast, constant, and convenient services, although with new risks in the form of threats to privacy, and cyberattack on consumers, and the bad reputation of the financial institution.

South African banks employ digital facilities such as quick-chat banking, robot advisers, intelligent depositor devices, video-banking, self-service kiosks, virtual reality, a grab-and-learn wall, and facial recognition, big data analytics, cloud computing, blockchain, AI, biometrics, and quantum computing in their branches (Capitec Bank Ltd, 2017; Nedbank Group Ltd, 2017; Standard Bank Group Ltd, 2016).

The integration of IT-based facilities into banking services has revolutionized banking operations but, with a significant increase in the occurrence of cyberfraud (Ali et al., 2017; Dzomira, 2017; Kshetri, 2019).

Table 10 shows the percentage responses obtained for the nature of the information security risks investigated in the South African banking industry. The responses are grouped under five major risk indicators, namely: breach of customers' information, breach of organisation's information, damage or loss of customers' sensitive information, damage or loss of organisation's sensitive information, and data leakage. The responses obtained indicated that the forms of information security identified in Table 10 occur sometimes or occasionally. This is displayed in Figure 6.

Table 10. Nature of the information security risks.

Nature of the information security risks	Percentage response (%) (Always)	Percentage response (%) (Often)	Percentage response (%) (Sometimes)	Percentage response (%) (Rarely)	Percentage response (%) (Never)	Total percent response (%)
Breach of customers' information	0	0	78.5	21.5	0	100
Breach of organisation's information	0	0	56.80	43.2	0	100
Damage or loss of customers' sensitive information	0	0	25.76	74.24	0	100
Damage or loss of organisation's sensitive information	100	0	22.34	77.66	0	100
Data leakage	100	0	26.21	73.79	0	100

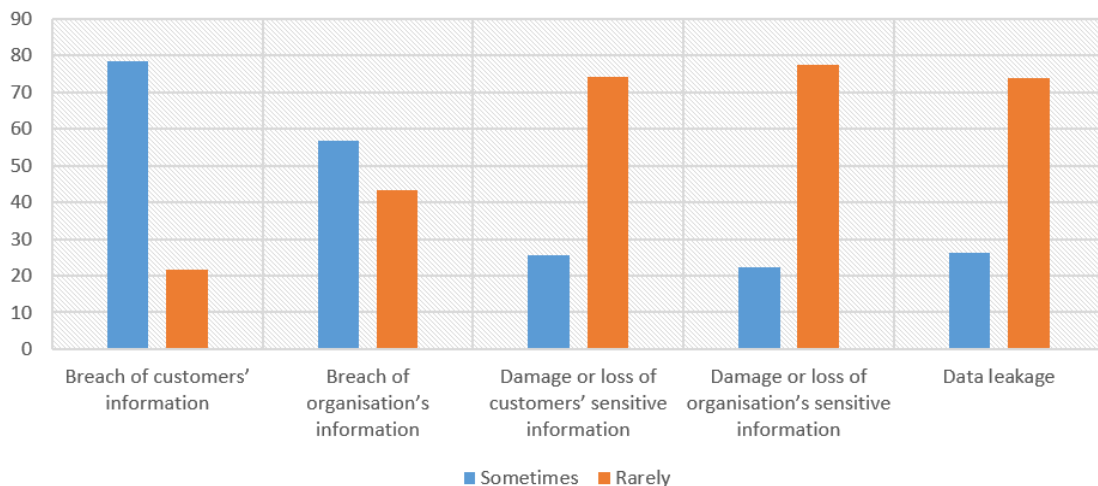


Figure 6. Nature of the information security risks.

Table 11 presents the Chi-square and Fischer's Exact statistics obtained for the nature of information security risks.

The results indicate that an independent relationship exists between the variables of breach of customers' information and damage or loss of customers' sensitive information. This is justified by the p -values of both the Chi-square and Fischer's Exact tests that were significant (level less than 0.05) at a 95% confidence level. This suggests that the pairs of identified factors are independent variables. Furthermore, the Spearman correlation coefficient indicates that the relationship between the two factors is negative but moderate. This implies that the higher the cases of breaches in customers' information, the lower the cases of damage or loss of customers' sensitive information. This implies that, despite the cases of breaches of customers' information, the confidential information of the customers may not be likely to be affected.

For the relationship between breach of organizations' information and damage or loss of organisations' sensitive information, it is evident to justify that a breach in an organisation's information may likely result in loss of organisation's sensitive information. Thus, the two variables may be dependent. This is justified by the p -values of both the Chi-square and Fischer's Exact tests that were significant (level greater than 0.05) at a 95% confidence level. This is supported by the Spearman correlation, which indicates the possibility of a positive but weak the relationship between the two variables. The results also show that the relationship between breaches of customers' information and data leakage may be dependent. This is justified by the p -values of both the Chi-square and Fischer's Exact tests that were significant (level less than 0.05) at a 95% confidence level. The Spearman correlation coefficient indicates that the relationship between the two factors is negative and weak. This implies that a breach in customers' information may result in minimal data leakage.

For the relationship between breaches of customers' information and data leakage, there was not sufficient evidence to justify the relationship between the two variables. The p -value for the Chi-square test (0.043) was close to 0.05, while the p -value for the Fischer's Exact tests (0.090) exceeded 0.05 at a 95% confidence level. The Spearman correlation coefficient indicates that the relationship between the two factors is negative and weak. This implies that an increase in the number of cases of breaches of customers' information might not result in data leakage.

For the relationship between a breach of organisation's information and data leakage, there was not sufficient evidence to justify the relationship between the two variables. The p -value of the Chi-square test (0.043) was close to 0.05, while the p -value for the Fischer's Exact test (0.506) exceeded 0.05 at a 95% confidence level. The Spearman correlation coefficient indicates that the relationship between the two factors is positive but weak. This implies that an increase in the number of cases regarding breaches of customers' information might likely result in an increase in cases of data leakage.

Finally, the result obtained for the relationship between breach of the organisation's information and damage or loss of customers' sensitive information shows that the two variables are independent. This is justified by the p -values of both the Chi-square and Fischer's Exact tests that were significant (level less than 0.05) at a 95% confidence level. Furthermore, the Spearman correlation coefficient indicates that the relationship between the two factors is positive but weak. This implies that the higher the number of cases is regarding breach of organisation's information, the higher the chances for damage to or loss of customers' sensitive information.

The survey results indicated that a breach in the confidential information of the organisation might be a result of the login details of the customers shared by the customers with unauthorised users. It could also be the consequence of clients using public or unprotected networks for banking operations, or poor password security detail. This is evident in the number of concurrent system logins with the same identity. Some respondents also traced the breach in customers' information to external attacks through spam emails, phishing, and malware attacks.

The improper security assignment as indicated by the user with similar roles but different security assignments may also imply a breach in the employee’s ethical conduct through unauthorised access to customers’ information. On the part of the organisation, a breach in organisation data could be traced to the employee’s breach of the ethical conduct through the sharing of organisation’s sensitive or system’s login credentials with unauthorised users. It was also traced to external attacks through spam emails, phishing, and malware attacks. Some respondents opined that an organisation’s database is subject to attack by threat actors in order to gain access to customers’ sensitive information.

The exposure of customers’ and organisations data or sensitive information to unauthorised persons as one of the major causes of data breaches can be tackled through customers’ sensitisation and the training of employees on ethical conduct.

Table 11. Chi-square and Fischer’s exact tests for nature of information security risks.

Variables	Chi-square statistics	Df	Asymp. sig.	Fischer’s exact sig.	Spearman’s correlation	Remarks
Relationship between breach of customers’ information and damage or loss of customers’ sensitive information	13.590	1	< 0.001	< 0.001	-0.569	Negative but moderate
Relationship between breach of organisations’ information and damage or loss of organisations’ sensitive information	1.992	1	0.158	0.258	0.218	Positive but weak
Relationship between breach of customers’ information and data leakage	4.087	1	0.043	0.090	-0.312	Negative and weak
Relationship between breach of organisation’s information and data leakage	0.622	1	0.0430	0.506	0.122	Positive but weak
Relationship between breach of organisation’s information and damage or loss of customers’ sensitive information	4.706	1	0.030	0.042	0.335	Positive but weak

Table 12 presents the summary of the responses obtained from the open-ended questions that relates to information security.

Table 12. The outcome of the open-ended questions and the problem solving questions.

S/No	Questions	Summary of responses
1.	What are the limitations impeding effective information security in your organisation?	According to the respondents, the following are the challenges hindering better information security in the banking sector: Inadequate training, that is, structures that can only be taken care of by equipped staff, management issues, human resources constraint, the system’s vulnerability and unauthorised intrusions, poor awareness and education, lack of available resources, administrative lapses, poor information dissemination, as well as inadequate system and personnel updates.
2.	How can the level of information security management in your organisation be described?	The respondents described the level of information security management as: “satisfactory”, “properly managed but there is room for improvement”, “average”, “high”, “effective” but can be improved”, “the banks are committed to a quality information management system, but improvement is necessary because of the rising occurrence of Cyberfraud in the sector.”
3.	What is the feasibility of integrating	Most of the respondents supported the integration of forensic

S/No	Questions	Summary of responses
	forensic accounting and management control systems as a technique for promoting information security in the South African banks?	<p>accounting and management control systems as a feasible tool for promoting information security in the banking sector. Below are their responses (views):</p> <ol style="list-style-type: none"> I. The integration, if well implemented, has the ability to stem the rate of Cyberfraud in the banking sector. II. The integration is a policy issue that requires the approval and collaboration of the bank stakeholders. III. Forensic accounting will succeed in fraud tracking once adequate information is provided by management control systems. IV. Employment of forensic accounting and management control experts will help to achieve this goal effectively. V. The integration alone is not sufficient; stakeholders need to work together across the banking sector to combat cyberfraud successfully (system uniformity). VI. The integration will limit the risk associated with cyberfraud.

5. DEVELOPMENT OF AN INTEGRATED INFORMATION SECURITY FRAMEWORK

Survey data has been used in the study to investigate the level of information security and its effectiveness in the South African banking industry. The results indicate that the level of effectiveness of information security on customers’ service in the South African banking industry is assumed to be high. However, the consequences of cyberfraud incidents for clients are severe. The South African banking industry has deployed some anti-fraud technologies that will be helpful in the implementation of forensic accounting and management control systems in this digital era. Thus, this study proposes an integrated information security framework that can be used to promote information security, as depicted in Figure 7. Hence, in a bid to promote information security, a forensic accountant may employ anti-fraud technologies as preventative strategies as part of the efforts geared to secure systems and data from cyberattack. In any event of cyberfraud, an initial forensic analysis can be carried out, including instant measures to recover the organisation’s system and prevent further intrusion into other sensitive information. A thorough forensic investigation will follow this in order to identify the fraud and the perpetrators (Kopp, Kaffenberger, & Wilson, 2017). The management control systems are able to assist in the testing and implementation of defence strategies to promote the organisation’s objective of information security (Otley, 2016). The control systems can also carry out performance measurement to ascertain that the strategies are implemented according to the organisation’s cyberfraud mitigation objectives.

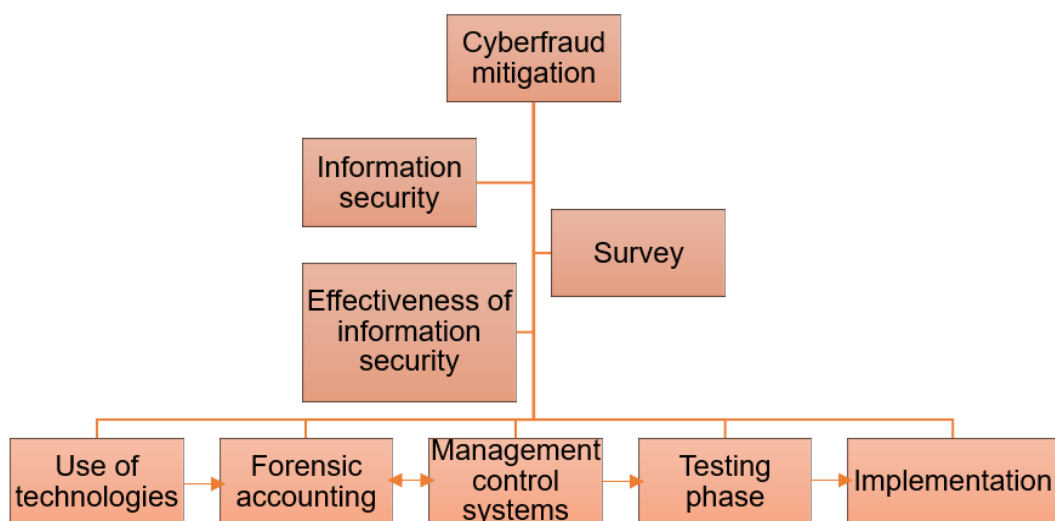


Figure 7. The implementation framework.

The results obtained from the survey also indicate significant intrusion and information breaches in the South African banking industry, thus the need for the information system's boundary identification and protection.

5.1. Information System's Boundary Identification

Information system's boundary will indicate the data storage location, the data flow, and its dependencies.

The organisation's management control systems will need to define the system's boundary in terms of the information resources allocated to it as well as the way the information resources are stored, processed, and transmitted. The components that link the information systems must also be identified. These may include security services, virtualization components, and servers such as web, application, database, Domain Name Systems and network components. Part of the management control system should also be directed towards the scope of the system's boundary. These may include the estimation and documentation of all the systems and applications used for data storage, processing, and transmission. The information system's boundary can be defined such that it will encompass the whole operating environment, directory services, e-mail, shared services, and Domain Name Systems. However, decision needs to be made on the scope of the boundary. When the information system's boundary is too small, such an organisation may face the risk of excluding critical resources from critical dependencies. This may have a negative impact on data protection, confidentiality, integrity, and availability. On the other hand, when the information system's boundary is too large, it could also be subject to external risks that are outside internal controls. Hence, a well-defined information system boundary that captures data storage, processing, and transmission will aid information security.

5.2. Information System's Boundary Protection

Having identified the scope of the organisation's information system and its components, the next step will be the development and implantation of strategies to safeguard it. The boundary protection strategies are to control and monitor the communications at the external boundary of the defined information system. The purpose of this is to identify and stop malicious communications and other types of intrusion. This can be achieved through the use of firewalls, routers, gateways, encryptions, and high-security zone devices, among others. The high-security zone devices can be employed to protect the boundary of the information systems, coupled with the protections offered at the organisation's level.

These devices can be integrated between the organisation's network and the internet, as well as the demilitarized zone. The demilitarized zone is a buffer zone that separates an organisation's local area network from an untrusted network, such as the public internet. This is an additional layer of security that can hinder threat actors access to the internal server and organisation's data. The demilitarized network may comprise an integrated router, webserver, and web mail that can be deployed between two firewalls, which separates an organisation's local area network from the public internet. This implies that a threat actor using a private or public network will break through the first firewall, and intrude into the demilitarized networks and then the second firewall before accessing organisations sensitive information. The demilitarized networks are usually equipped with real-time alerts to warn organisation's security personnel of an impending intrusion. Furthermore, the information system's boundary protection may also comprise four major aspects, namely authentication, policy management, application security, and system and network administration. Policy management caters for the implementation of the organisation's strategies for information system's boundary protection, such as authentication, while applications security checks for the system's vulnerabilities. The system and network administration deals with the organisation, installation, and management of an organisation's data communication systems and networks to ensure their functionality.

6. CONCLUSION AND IMPLICATIONS

The purpose of this study is to explore the level of information security in the South African banking industry. This was achieved via a mixed method involving quantitative and qualitative approaches, which involves data collection with the use of a structured questionnaire and hypothesis testing. The results obtained indicate that the level of effectiveness of information security on customers' service in the South African banking industry is assumed to be high. South African banks are deploying different technologies to strengthen the level of information security; however, there are still substantial cases of cyberfraud and unauthorised intrusions. The implication of an information security breach, as established by the hypotheses tested, is evidenced by the increase in information security risks and number of cyberfraud cases in the banking industry, which greatly affect customers. This may make customers lose confidence in the products and services offered by the banks. The results obtained from the hypothesis testing indicate that the integration of forensic accounting and the management control system may be a useful tool for tackling cyberfraud, thereby ensuring customers' satisfaction through an improved information security system. In view of the findings in this study, a management solution comprising an integrated information security framework can consolidate information security in the banking industry. As part of management control measures to promote information security, it is recommended that the security systems be upgraded to provide real-time assessments of breaches in security and regulatory requirements. One of the limitations of this study is that the survey is mostly qualitative in nature, without actual figures on incidences of information and data breaches. Secondly, the developed integrated security framework is limited to the conceptualised phase. Thus, future work can investigate the success of the anti-fraud technologies employed for managing information security in the South African banking industry using a mixed-method approach and the validation of the developed information security framework.

Funding: This study received no specific financial support.

Institutional Review Board Statement: The Ethical Committee of the Tshwane University of Technology, South Africa has granted approval for this study on 10 May 2020 (Ref. No. FREC 2020/004-ECO).

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

- Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security*, 5(1), 118-131.
- Akelola, S. (2012). Fraud in the banking industry: A case study of Kenya Published PhD Thesis in the School of Business. In (pp. 1-422). UK: Nottingham Trent University.
- Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020a). Analysis of cyber-crime effects on the banking sector using the balanced 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), 1253-1271. <https://doi.org/10.1108/jfc-04-2020-0053>
- Alabdullahi, T. T. Y., Alfadhi, M. M. A., Yahya, S., & Rabi, A. M. A. (2013). The role of forensic accounting in reducing financial corruption: A study in Iraq. *International Journal of Business and Management*, 9(1), 26-34. <https://doi.org/10.5539/ijbm.v9n1p26>

- Ali, L., Ali, F., Surendran, P., & Thomas, B. (2017). The effects of cyber threats on customer's behaviour in e-banking services. *International Journal of e-Education, e-Business, e-Management and e-Learning*, 7(1), 70-78. <https://doi.org/10.17706/ijeeee.2017.7.1.70-78>
- Böhme, R., & Moore, T. (2012). *How do consumers react to cybercrime?* Paper presented at the eCrime Researchers Summit (eCrime), Proceedings of the 7th IEEE APWG eCrime Researchers Summit (eCrime) Las Vegas.
- Capitec Bank Ltd. (2017). *Integrated annual report*. Retrieved from https://www.capitecbank.co.za/globalassets/pages/investor-relations/financial-results/2017/annual-report/integrated_annual_report.pdf
- Carenys, J. (2012). Management control systems: A historical perspective. *International Journal of Economy, Management and Social Sciences*, 1(1), 1-18.
- Centre for Excellence in Financial Service. (2017). *The impact of the 4th industrial revolution on the South African financial services*. Retrieved from <https://coefs.org.za/impact-4th-industrial-revolution-south-african-financial-services-market/>
- Chi-Chi, O. A., & Ebimobowei, A. (2012). Fraudulent activities and forensic accounting services of banks in Port Harcourt, Nigeria. *Asian Journal of Business Management*, 4(2), 124-129.
- Choobineh, J., Dhillon, G., Grimaila, M. R., & Rees, J. (2007). Management of information security: Challenges and research directions. *Communications of the Association for Information Systems*, 20(1), 958- 971. <https://doi.org/10.17705/1cais.02057>
- Cusack, B., & Ahokov, T. (2016). *Improving forensic software tool performance in detecting fraud for financial statements*. Paper presented at the In Valli, C. (Ed.), 2016, 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*. Paper presented at the The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013). Kuala Lumpur, Malaysia, 4 - 6 March, 2013.
- 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. (2017). Internet banking fraud alertness in the banking sector: South Africa. *Banks and Bank Systems*, 12(1), 143-151. [https://doi.org/10.21511/bbs.12\(1-1\).2017.07](https://doi.org/10.21511/bbs.12(1-1).2017.07)
- Finau, G., Samuwai, J., & Prasad, A. (2013). Cyber crime and its implications to the pacific. *The Fiji Accountant*, 2013(June), 15-16.
- Gebremeskel, B. K., Jonathan, G. M., & Yalew, S. D. (2023). Information security challenges during digital transformation. *Procedia Computer Science*, 219, 44-51. <https://doi.org/10.1016/j.procs.2023.01.262>
- Georgili, E., & Pitsi, E. (2022). *Cybersecurity in the new era: A view from Greece Kyriakides georgopoulos law firm*. Retrieved from <https://kglawfirm.gr>
- Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, 46(7), 404-410. <https://doi.org/10.1016/j.im.2009.06.005>
- Henri, J.-F., & Journeault, M. (2010). Eco-control: The influence of management control systems on environmental and economic performance. *Accounting, Organizations and Society*, 35(1), 63-80. <https://doi.org/10.1016/j.aos.2009.02.001>
- Holappa, J., Ahonen, P., Eronen, J., Kajava, J., Kaksonen, T., Karjalainen, K., . . . Savola, R. (2005). *Information security threats and solutions in digital television: The service developer's perspective*. VTT electronics research notes 2306. Retrieved from <https://www.vttresearch.com/sites/default/files/pdf/tiedotteet/2005/T2306.pdf>
- Jaishankar, K. (2008). Space transition theory of cybercrimes in schmallager, F., & Pittaro, M. (Eds.), *Crimes of the internet*. In (pp. 283-301). Upper Saddle River, NJ: Prentice Hall.
- Jhawar, R., & Piuri, V. (2017). Fault tolerance and resilience in cloud computing environments. In *computer and information security handbook*. edited by J.R. Vacca, Elsevier, Morgan Kaufmann Imprint. In (pp. 165-181). United States: Morgan Kaufmann.
- Kadiri, K. O. (2014). The prospects and problems of information technology in the banking sector in Nigeria. *IOSR Journal of Computer Engineering*, 16(5), 28-35.

- Khan, M., & Barua, S. (2009). The status and threats of information security in the banking sector of Bangladesh: Polices required. *Bangladesh Journal of Management Information System*, 1(2), 1-27.
- Ko, M., & Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: An empirical investigation. *Journal of Information Technology Management*, 17(2), 13-22.
- Kong, H., Jung, S., Lee, I., & Yeon, S. J. (2015). Information security and organizational performance: Empirical study of Korean securities industry. *ETRI Journal*, 37(2), 428-437. <https://doi.org/10.4218/etrij.15.0114.1042>
- Koo, J. M., Park, J. S., & Park, J. H. (2013). Study about the impact of information security systems on corporate performance: Based on IT relatedness theory. *Asia Pacific Journal of Information Systems*, 23(4), 129-149. <https://doi.org/10.14329/apjis.2013.23.4.129>
- Kopp, E., Kaffenberger, L., & Wilson, C. (2017). *Cyber risk, market failures, and financial stability*. IMF Working Paper No. 17/185.
- Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change*, 80(3), 541-555. <https://doi.org/10.1016/j.techfore.2012.07.002>
- Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, 22(2), 77-81.
- Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, 45, 58-74. <https://doi.org/10.1016/j.cose.2014.05.006>
- Lee, M., & Lee, J. (2012). The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet. *Information Systems Frontiers*, 14(2), 375-393. <https://doi.org/10.1007/s10796-010-9253-1>
- Maglaras, L., Drivas, G., Chouliaras, N., Boiten, E., Lambrinouidakis, C., & Ioannidis, S. (2020). *Cybersecurity in the era of digital transformation*. Paper presented at the The Case of Greece 2020 International Conference on Internet of Things and Intelligent Applications, Zhenjiang, China, IEEE.
- Malik, M. S., & Islam, U. (2019). Cybercrime: An emerging threat to the banking sector of Pakistan. *Journal of Financial Crime*, 26(1), 50-60. <https://doi.org/10.1108/jfc-11-2017-0118>
- Martin, N., & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security*, 30(8), 803-814. <https://doi.org/10.1016/j.cose.2011.07.003>
- Mbeli, 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 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing, Beijing.
- Mohammeda, H. K., & Knapkova, A. (2016). The impact of total risk management on company's performance. *Procedia-Social and Behavioral Sciences*, 220, 271-277.
- Nedbank Group Ltd. (2017). *Integrated annual report*. Retrieved from <https://www.nedbank.co.za/content/dam/nedbank/site-assets/AboutUs/Information%20Hub/Integrated%20Report/2017/2017%20Nedbank%20Group%20Integrated%20Report.pdf>
- Network Encyclopedia. (2023). *Importance of cyber security in the digital era*. Retrieved from <https://networkencyclopedia.com/importance-of-cyber-security-in-the-digital-era/#:~:text=The%20goal%20of%20cybersecurity%20is,and%20even%20cause%20physical%20harm>
- Obeng-Adjei, A. (2017). *Analysis of cybercrime activity: Perceptions from a South African financial bank a research report*. Masters' Thesis, University of Witwatersrand, South Africa, pp. 1-87.
- Okoye, E., & Akamobi, N. L. (2009). The role of forensic accounting in fraud investigation and litigation support. *The Nigeria Academic Forum: A Multidisciplinary Journal*, 17(1), 39-44.
- Oppenheim, A. N. (1992). *Questionnaire design, interviewing and attitude measurement*. London: Pinter.
- Otley, D. (2016). The contingency theory of management accounting and control: 1980–2014. *Management Accounting Research*, 31, 45-62. <https://doi.org/10.1016/j.mar.2016.02.001>
- Peikari, H. R. (2010). *The influence of security statement, technical protection, and privacy on satisfaction and loyalty; a structural equation modeling in global security, safety, and sustainability*. Paper presented at the International Conference, ICGS3 2010, Braga, Portugal, September 1-3, 2010. Proceedings 6 Springer Berlin Heidelberg.

- Perdub, V. V., Ceklic, J., & Ceklic, B. (2018). The role of forensic accounting in corporate governance for economic studies. *Poslovne Studije, Business Studies*, 10(19-20), 119-131.
- Rao, H. S. (2019). Cybercrime in banking sector. *International Journal of Research - Granthaalayah*, 7(1), 148-161.
- Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence*, 2(3), 1-28.
- Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, 2(2), 202-209.
- Sattarova Feruza, Y., & Kim, T. H. (2007). IT security review: Privacy, protection, access control, assurance and system security. *International Journal of Multimedia and Ubiquitous Engineering*, 2(2), 17-32.
- Serhii, K., Vadym, P., Oleg, K., Oleksandr, M., & Strilets, O. (2019). Forensic economic examination as a means of investigation and counteraction of economic crimes in East Europe example of Ukraine. *Journal of Legal, Ethical and Regulatory Issues*, 22(3), 1-8.
- Shrivastava, A. K. (2016). The impact assessment of IT infrastructure on information security: A survey report. *Procedia Computer Science*, 78, 314-322. <https://doi.org/10.1016/j.procs.2016.02.062>
- Skalak, S., Alas, M. A., & Sellito, G. (2011). Fraud: An introduction in a guide to forensic accounting investigation edited by Golden Thomas, W., Skalak, Steven, L., and Mona, M. Clayton. In (pp. 1-23). Hoboken, NJ: John Wiley and Sons. Inc., US.
- Slavoljub, S., Srdjan, S., & Predrag, V. (2015). Management control in modern organisations. *International Review*, 3(4), 39-49.
- Standard Bank Group Ltd. (2016). *Report to society*. Retrieved from https://www.standardbank.com/static_file/StandardBankGroup/filedownloads/archives/Report-to-Society-2016.pdf
- 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>
- Tekavčič, M., & Peljhan, D. (2003). Insights into managerial tools related to cost management in Slovenian companies. *Zbornik radova Ekonomskog fakulteta u Rijeci: časopis za ekonomsku teoriju i praksu*, 21(1), 83-97.
- Tiwari, S., Bhalla, A., & Rawat, R. (2016). Cybercrime and security. *International Journal of Advanced Research in Computer Science and Software Engineering*, 6(4), 46-52.
- United Nations Office on Drug Crime. (2013). *Comprehensive study on cybercrime United Nations UK*. Retrieved from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
- Usher, A. (2006). *Essential strategies for protecting against the new wave of information security threats sharp ideas LLC*. Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKewiyn67lsN7sAhXOSxUIHV PoB9wQFjAAegQIAxAC&url=http%3A%2F%2Fwww.sharp-ideas.net%2Fdownload%2Femerging_security_threats.ppt&usg=AOvVaw2ntWRMH_QSQnom4WqnS6_E
- Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. *The African Journal of Information and Communication*, 20, 113-132. <https://doi.org/10.23962/10539/23573>
- Wells, J. T. (2003). The fraud examiners. *Journal of Accountancy*, 196(4), 76-80.
- Wilson, N., & McClean, S. (1994). *Questionnaire design: A practical introduction university of Ulster copies available from: UCoSDA, level six, university house*. Sheffield: University of Sheffield.

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.