Heliyon 8 (2022) e12054

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

The use of the Balanced Scorecard as a strategic management tool to mitigate cyberfraud in the South African banking industry

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

Faculty of Economics and Finance, Tshwane University of Technology (TUT), South Africa

ARTICLE INFO

Keywords:
Cyberfraud
BSC perspectives
Performance measurement
Strategic management and control framework

ABSTRACT

The main objective of this study is to employ the four perspectives of the Balanced Scorecard (BSC) for the analysis of cyberfraud in the South African Banking industry. In addition, this study develops a BSC strategic management control framework for mitigating the effect of cyberfraud in the South African Banking industry. To achieve these objectives, a qualitative approach involving the use of a structured questionnaire for data collection was used. The structured questionnaire made available to the staff of 17 licensed banks in South Africa in charge of management, administration and operations sections. Then the four perspectives of BSC i.e., the financial, internal business processes, customer as well as learning and growth perspectives were captured. The analysis of the responses obtained from primary data was carried out using a bar chart, and this led to the development of a BSC strategic management control framework for mitigating the effects of cyberfraud. The findings from this study show that the customer perspective, has 90.47% percent response from the indicators followed by learning and growth which relates to the employees (85.71%). The internal business processes are ranked in the third position with 57.26% while the financial perspective has the least with a percent response of 39.97%. This implies that the South African banking sector pays more attention to the non-financial than the financial measures. The implementation of the proposed BSC framework may help to promote cyberfraud reduction, improve management control systems, performance measurements, as well as customers' and shareholders' satisfaction.

1. Introduction

Globally, cyberfraud is the second most reported economic crime affecting organisations (PwC Global Economic Crime Survey, 2016:1). According to the PwC Global Economic Crime Survey (2016:1 & 2) about half of the organisations surveyed opined that local law enforcement agency is not resourcefully engaged for economic crime investigation, thus, leaving the onus on the organisations to fight crime (PwC Global Economic Crime Survey, 2016:1 & 2). Cyberfraud has been reported to be a serious threat and have implications on South African organisations due to a lack of suitable blueprints to counter such incidences (PwC Global Economic Crime Survey, 2016:1 & 2).

Kaplan and Norton (1992) opined that the role of finance was critical in the ancient performance measurement system. Thus, financial measures seemed to be more important than non-financial ones (Chenhall and Langfield 2007:266; Betianu and Briciu, 2011:20). That is why the BSC by Kaplan and Norton captures both financial and non-financial measures to address the limitations of the conventional accounting systems and to prevent performance measurement from over-dependence on financial indicators (Kaplan and Norton, 1992; Ittner and Larcker, 1998:205). Therefore, the BSC includes three additional perspectives: internal business processes, customer, and innovation (learning and growth). It also comprises outcome measures as well as respective performance drivers, which are interconnected in a cause-and-effect relationship (Kaplan and Norton, 1996a: 53, 76; Kaplan and Norton, 1996b:31).

The motivation for this study is to unpack South Africa's continued highest instances of economic crime in the world over the past decades (2008–2017) (PwC Report, 2018:6) using the four perspectives of Balanced Scorecard (BSC). Even though the economic crime rate in South Africa dropped from 77% to 66% in 2020 (PwC Report, 2020:8), it still remains higher than the global average rate (47% in the same year; PwC Report, 2020:8). In line with this, cyberfraud is reportedly increasing in the banking industry in South Africa with phishing being on the top list of the online fraud (Cassim 2016:130). In 2019, the number of incidences increased to 26 567 and in 2020 even 35 308, reportedly costing the banking industry about R308 million in 2019 and R309 million in gross losses in 2020 respectively (SABRIC, 2020).

* Corresponding author.
E-mail address: Oluwatee01@gmail.com (O. Esther Akinbowale).

https://doi.org/10.1016/j.heliyon.2022.e12054
Received 7 April 2022; Received in revised form 12 August 2022; Accepted 24 November 2022

Putting the focus on the financial and non-financial measures in the South African banking industry, the main objective of this study is to develop a BSC strategic management control framework for mitigating the effects of cyberfraud in the South African banking industry, employing the four perspectives of the Balanced Scorecard (BSC).

In order to address this objective, two research questions were formulated as follow:

1. What is the focus of the South African banking sector with respect to the four BSC perspectives and cyberfraud mitigation?
2. What is the potential of the BSC perspectives in relation to the measurement and control system for the banking sector in the quest to mitigate cyberfraud?

The implementation of the proposed BSC framework using qualitative analysis may help organisations to identify some potential risks that can result in cyberfraud incidences. It can also aid the fraud risk management processes (risk identification, assessment and mitigation). This includes the identification of the perpetrators, scope of fraud as well as the internal controls that have been compromised or violated. Hence, the remaining sections of this paper are organised as follows: chapter 2 presents the overview of selected literature review which details on the context of the South African banking sector, cyberfraud incidences and the Balanced Scorecard (BSC). Next to this section is the methodology. Section four presents the results, and the discussion leads to the framework, before the study gets concluded.

2. Literature review

2.1. The South African banking industry

The well-developed South Africa banking industry, overseen by the South Africa Reserve Bank (SARB), is well-positioned and has similar standards as the financial sectors in many advanced nations (SARB, 2020; Moyo, 2018:3; South African Banking Report, 2019). For instance, in 2010, it was ranked 6th out of 133 countries in relation to the safety of banking operations and sophistication of its financial market (Coovadia, 2011:6). By the end of 2017, total assets of R5.14-trillion (representing 91% of them) were domiciled with the five largest banks. However, the Bank Supervision Department of the South African Reserve Bank, stated that there are even 75 commercial banks operational in South Africa: 42 foreign banks representatives, 14 branches of foreign banks, 10 locally controlled, 6 foreign controlled banks and 3 mutual banks (www.resbank.co.za). Regardless of the fact that there are various banks under different categories, there are only four major banks controlling over 80% of the banking industry: First National Bank (FNB), Amalgamated Bank of South Africa Limited (ABSA) Standard Bank, and Nedbank (Banking Association of South Africa, 2015).

In the South Africa banking industry, digital solutions, cost-effective operational frameworks as well as supply-chain integration have been the highest management priorities (PwC Report 2019:4). The non-traditional stakeholders now subscribe to these emerging trends to provide in-house banking solutions to customers (PwC Report 2019:4). Furthermore, with respect to the rising cyberfraud risk in the banking industry, the 'four major banks' (as mentioned above) are gradually developing novel approaches such as data mining and digital transformation to ensure a steady market relevance, technological and regulatory compliance, improved competitiveness and effective customers' service (PwC Report 2019:4). In addition to this, since these banks hold the major portion of the South Africa's banking business and have most of the customers, there is a need for the development of robust cyber and information technology (IT) resilience and data analytical competencies for data analysis and new ways to meet the customers' need (PwC Report 2019:4).

2.2. Cyberfraud

Fraud is an illegal action marked by deception, an attempt to conceal, or trust violation etc (Institute of Internal Auditors, 2009:4). These acts are not a function of the threat of violence or physical force. In the same sense, Ramamoorti et al. (2014:47) maintain that it is an act of purposeful intention to deceiving another party with intensity of desire, and possibility of apprehension, including violation of trust and rationalization. According to Idolor (2010:62), it also involves theft and falsification of accounting records often complemented with an attempt to conceal or convert stolen assets into personal assets. These accounting records encompass all the books and documentations used for preparing financial statements, or those important to financial reviews and audits. Besides these, they also comprise of the records of assets and liabilities, financial transactions, invoices, cheques, journals and ledgers etc. Fraud is a global phenomenon affecting virtually all the continents and impacting all the sectors of the economy, and it can be perpetrated by parties and organizations to gain money, property, services or to avoid payment or loss of services (Bhasin, 2016:200). Furthermore, fraud can impact organizations negatively not only limited to financial, operational, or reputational spheres; losses can be significant not only financially, but also in form of reputation, goodwill, and customer relations (Bhasin, 2011:34). In the context of financial reporting, fraud has been defined as an intentional effort of misleading or deceiving in particular the stakeholders, but also other readers of published financial statements, through the preparation and dissemination of misstated financial statements (Rezaee, 2005: 279).

Cyberfraud covers various crimes, often carried out by using false identities to deceive and swindle their clients. Such crimes are carried out with the aid of information technology infrastructure and through global electric networks, internet, and other IT devices and can affect individual or corporate data and systems (e.g. hacking), or relate to computer-related forgery (like phishing), content (as in the case of distributing child pornography), and copyright crimes (like circulating pirated contents) (KPMG, 2011:4; Jegede, 2014:13; Tiwari et al., 2016:46; Monni and Sultana, 2016:13; Meephlam, 2017:17; Okeshola and Adeta, 2013:98).

Unfortunately, due to the higher complexity of and time consumption for investigating and prosecuting cyberfraud, it often needs to be treated differently than conventional fraud (Clayton, 2011:271). Kshetri (2019:77) noted that cyberattack incidences are increasing swiftly in emerging economies (Kshetri, 2019:77), one of the reasons attributed to the recent advances in information technology (Ali et al., 2017:70). Unethical endeavours and crime characterize big parts of the cyberspace, contributing to the increasing rate of cyberfraud over the years (Uma and Padmavathi, 2013:392). The misuse of the cyberspace for activities as unauthorised intrusions into individual and corporate information, and other forms of fraud such as fiscal fraud, spying, disruption of networks, generation of fake links, impersonation, data theft, cash theft, malware attacks, ATM fraud, cyber money laundering, credit card fraud, IP theft, and online fraud etc. has severe implications on the customers, financial institutions, and the public at large (Detica, 2011:1; Raghavan and Parthiban, 2014:176; Dzomira, 2014:17). It was estimated that the annual cost of cybercrime occurrences on the global economy was more than $400 billion with the conservative and maximum estimates in losses pegged at $375 billion and $575 billion respectively (Centre for Strategic and International Studies, 2014). The South African Banking Risk Information Centre (SABRIC, 2019) stated the total number of cybercrime incidences as 13 438 for the year 2017. These cases include fraud committed via mobile and banking apps as well as online platforms with damages to the banking sector reported beyond R250 000 000 in total. This calls for the introduction of powerful solutions capable of curbing cyber-threats and to minimise the consequences posed by cyber-fraud. Hence, in the fight against cybercrime, the strategy of the financial institutions should include effective measurements in their approach for

management control. Although many works have been reported on the application of BSC for strategic planning or as a management control tool in organisations, there is still a dearth of information regarding the implementation of BSC as a strategic management and control tool for cyberfraud mitigation. Yang and Lee (2020) developed a strategic map for forensic accounting which incorporates the fraud risk management controls. To achieve this, they employed an integrated BSC based decision framework which presents information relating to key indicators necessary to achieve strategic planning, forensic accounting implementation and risk management in an organisation. Thus, and in extension to this, this study develops a BSC strategic management and control framework for mitigating the effect of cyberfraud in the banking industry.

2.3. Balanced scorecard

The Balanced Scorecard (BSC) originated from Kaplan and Norton (1992) as a technique for organisational performance measurement based on four perspectives, viz: financial, internal business processes, customer, as well as innovation and learning perspectives (also referred to as "learning and growth"; Kaplan and Norton, 2006a:54). The BSC is used for performance measurement and provision of financial and nonfinancial feedback to the organisations (Kaplan and Norton, 1996a:55). It has evolved from a performance measurement system into a strategic management system (Kaplan and Norton, 1996a:55). The use of BSC as a performance management tool and for the implementation of organisational strategies in commercial banks has been reported (Zhang and Li, 2009:209; Wu et al. 2010:695; Öztürk and Coskun, 2014:151; Stojkovski and Nenovski, 2021:1629).

Although its limitations such as rigidity, linearity, and focuses on individual organisation were identified (Voelpel et al., 2006:49–51), if properly deployed, it may assist organisations to achieve effective performance measurement and management control (Kaplan, 2001:357; Niven, 2002:301; Hogget et al., 2012:560). Nevertheless, the implementation of BSC requires management support and financial investment. Its process can get complicated, hence, the need for effective planning to tailor it to the organisation's needs (Niven, 2006:57; Primer, 2016:38–39).

In the context of this study, the implementation of the BSC framework may help to promote cyberfraud reduction, improve management control systems, performance measurements, as well as customers' and shareholders' satisfaction. To reach this target, a BSC strategic management and control framework can be developed to aid the process of cyberfraud mitigation. It can also be employed as a strategic tool to balance the financial and non-financial measures in an organisation.

3. Research design and methodology

The population used for this study consists of some selected experts from all the 17 licensed commercial banks listed in South Africa (Bankscope, 2018). The selected experts included in this study ensure good representation of the respondents since inadequate representation may affect the reliability and validity of the outcome of the survey (Fincham, 2008:2). This research employed purposive sampling because it permits the selection of specific groups possessing the necessary experience and expertise to understand the cyberfraud: key organisational staff, specifically involved in combating fraud and making decisions on management control systems to obtain comprehensive data on the expended and ongoing efforts to combat cyberfraud in the organisation. At least two participants, but mostly three participants were selected to participate in responding to the questionnaire across the 17 banks, making a total of forty-two participants. Figure 1 summarises the research design employed for achieving the aim of this study.

As shown in Figure 1, the qualitative approach was employed since it can assist in the understanding of multifaceted occurrences such as cyberfraud. Furthermore, it can explore the research problem from the perspectives, feelings and experiences of the stakeholders (Ospina, 2004:1279; Mohajan 2018:21 & 24). In order to do so, it involved the use of a structured open-ended questions as they allow to capture the perception of experts concerning sensitive issues like cyberfraud (Wilson and McClean, 1994) – in particular, to express their opinions about cyberfraud and the mitigation approaches employed by their respective organisations.

Whittemore (2001:522) indicated that the reliability of qualitative approach can be validated using certain criteria such as credibility, authenticity, criticality and integrity. These four criteria were ensured in the course of this study:

- Credibility: The information presented as the outcome of the survey is a precise interpretation of the different experts' opinion on cyberfraud and the mitigation approaches in the South African banking sector.
- Authenticity: The various opinions of the experts were captured and presented.

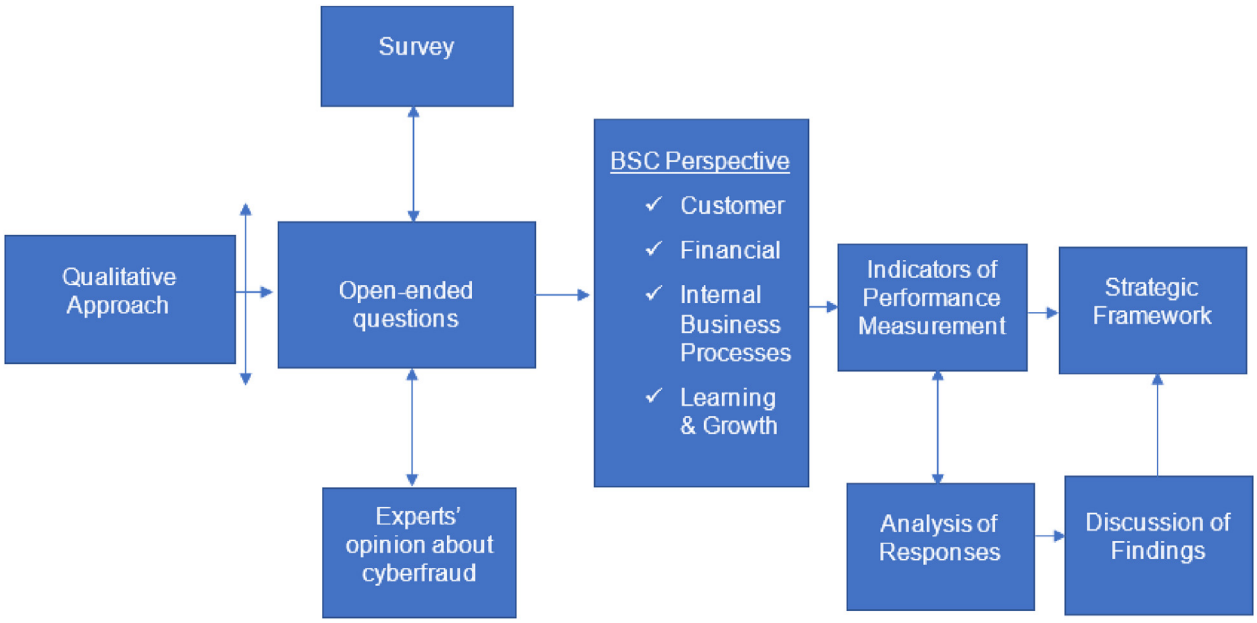

Figure 1. Research design. Source: Authors' synthesis

- Criticality: There was consideration of all the major aspects of this study (cyberfraud and the mitigation approaches in the South African banking sector).
- Integrity: The conduct of the research was in conformity with ethical practices. Ethical clearance was obtained from Research Ethics Committee of Tshwane University of Technology before the administration of the questionnaire.

The structured questionnaire completed by the selected staff of 17 licensed banks in South Africa responsible for operations, management, and administration captured all the four BSC perspectives. The analysis of the responses obtained from the questionnaire was carried out using a bar chart (depicted in Figure 2), and this led to development a BSC strategic management control framework for mitigating the effect of cyberfraud. Furthermore, the BSC was used to assist management make decisions on the spate of cybercrime considering four perspectives: internal, customers', financial, and innovation (learning and growth). Based on this, a Strategy Management System (SMS) enhanced by the BSC was developed for the decision-making process. The next section presents results and discussion based on the methodology employed in this section.

4. Results and discussion

4.1. Outcome of the survey: application of the BSC perspectives

This section addresses the first research question referring to the focus of the South African banking sector with respect to the four BSC perspectives and cyberfraud mitigation.

The BSC perspective was employed for the analysing the effect of cyberfraud on the South African Banking sector. Primary qualitative data were collected from the banks and the focus of the banks in terms of the four BSC perspectives was analysed using the four BSC perspectives. The four perspectives captured in the questionnaire completed by the South African banking staff in charge of management, operations, and administration as well as the indicators are summarised in Table 1, the received rate of answers from the 42 respondents with respect to the four BSC perspectives in Figure 2.

The results reflected in Figure 2 show that the customer perspective has 90.47% percent response from the indicators stated in Table 1 above, followed by learning and growth which relates to the employees (85.71%). The internal business processes are ranked third with 57.26% while the financial perspective has the least with a response rate of 39.97%. These results also indicate that the South African banking sector puts significant efforts into the reduction of the effect of cyberfraud on the customers and that the sector is investing in the development of human capacity to reduce cyberfraud. This led to more successfully blocked cyberattacks, additional operational time for the organisation's ICT systems, higher confidentiality of customers' or corporate information as well as improved integrity and maintenance of the information stored on the organisation's systems. However, cyberfraud has still negatively impacted the banking sector's revenue.

In the end the received answers also indicate that the South African banking sector focusses more on the non-financial than the financial measures. This may be a consequence of the effect of non-financial measures on the customers' and employee satisfaction or of poor internal business processes on the financial performance of an organisation. This result agrees significantly with the results of Georgiev (2017:59) as well as Rafiq et al. (2020:1), and Akinbowale et al. (2020). For example, Georgiev (2017:59) found out that the intangible capital of the organisation is more important and essential than the physical capital, while Rafiq et al. (2020:1) recognised greater consequences of the non-financial measures on employees' performance, unlike the financial performance measure. In the same way, the outcome of the literature review carried out by Akinbowale et al. (2020:956) indicates that financial institutions focus more on the customers' perspectives than

Table 1. BSC perspectives applied to the survey data.

Strategic objectives	Indicators
Financial	• Fiscal fraud, cash theft, ATM fraud, cyber money laundering, credit card fraud, fraudulent reimbursement, payroll fraud • Loans • Wire transfer
Customer	• More successful blocking of cyberattacks • Increased operational time for the organisation's ICT systems • Higher confidentiality of customers' or corporate information • Integrity and maintenance of the information stored on the organisation's systems
Internal Business Processes	• Internal controls by management, good organisation culture, and good ethical culture • Accountability, and adequate documentation/record keeping
Learning and Growth	• Use of new technology

Source: Authors' synthesis.

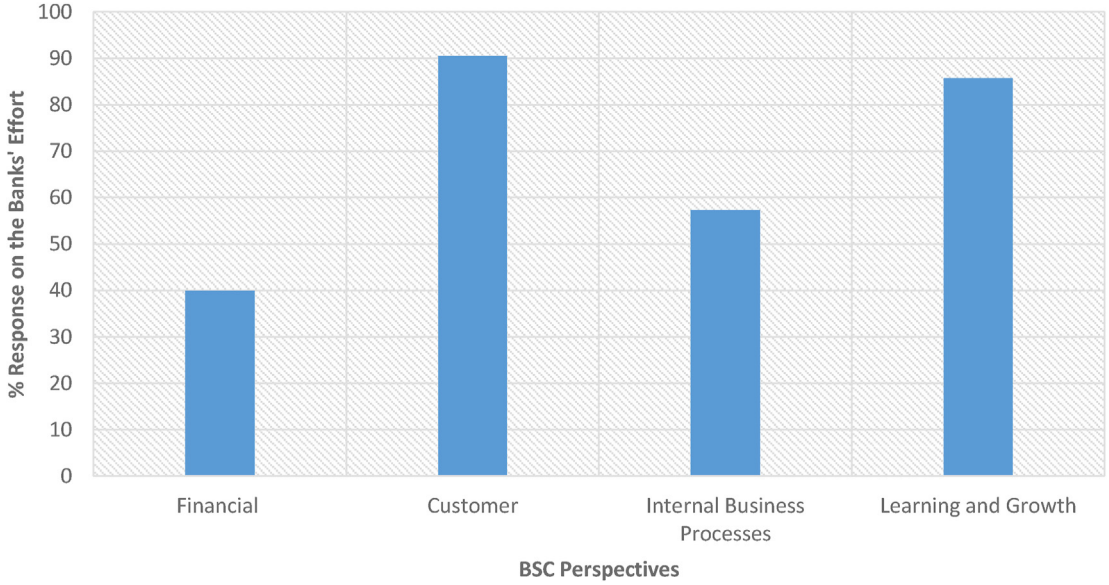

Figure 2. The bar chart showing percent response of the banks' effort from the four BSC perspectives. Source: Analysis of the survey data

other the three ones. Drucker (2007:31–32) explains this by the fact that the existence of any organisation is ultimately hinged upon the need to serve the need of customers, the success of such organisation being partly a function of the continuous patronage by customers. Hence, it is also a critical perspective among the BSC perspectives which should be prioritised, and Figure 2 confirms this for the banking industry.

4.2. BSC perspectives for measurement and control system for the banking sector

This section addresses the second research question referring to the potential of the BSC perspectives in relation to the measurement and control system for the banking sector in the quest to mitigate cyberfraud.

The BSC breaks an organisation's strategy down into different objectives, measured in four perspectives: customer, financial, internal business processes and innovation (learning and growth) (Kaplan and Norton, 1996b:30; Norreklit, 2000:67; Niven, 2005; Norreklit and Mitchell, 2007). Therefore, the BSC may also be used to assist management in making decisions on the spate of cybercrime considering the four perspectives: internal, customers, financial as well as learning and growth. Based on this, a Strategy Management System (SMS) enhanced by the BSC can be developed for making management decisions involving the following stages: problem identification, strategy formulation, derivation of action plans, alignment of plans with the organisation's objectives, planning of operations, monitoring and learning as well as validation and adaptation of the developed strategy. This leads to the process flow diagram in Figure 3 as well as the decision making and management system as presented in Figure 4 respectively.

Figure 3 is a practical guided approach that can assist organisations to effectively combat cyberfraud using BSC for both strategic management as well as controls. The steps presented are procedural namely: problem identification, development of strategy, translation of strategy into action plans, communication, alignment of action plans, planning, setting of targets, strategic feedback, review or leaning, monitoring as well as testing and adoption of the developed strategy.

The first step indicated in Figure 3 is the problem identification which in this case is cybercrime. The understanding of the nature of cybercrime, perpetrators and effects will foster the development of an effective strategy to mitigate it. With respect to cyberfraud mitigation, Prabowo (2011:378) explains that the formulation and implementation of sound strategies that can drive fraud prevention policies, internal controls, risk management, fraud awareness, implementation of anti-fraud technologies and legal deterrence are required in the prevention of cyberfraud occurrences. Hence. the gathering of the necessary information about cyberfraud is the first step in strategy formulation (Prabowo, 2011:375 & 382); the execution of a problem-based fraud prevention strategy can promote efficient resources utilisation for cyberfraud mitigation in a cost-effective manner.

The following translation of strategy to actions plans is necessary to ensure that the BSC targets are met (Niven, 2006:22). This is followed by effective communication. The evolution of the BSC as a communication tool from a measurement system is possible with the aid of a strategic map for effective communication of the organisation's strategy to the stakeholders, helping to mitigate the risks associated with cyber security (Niven, 2006:17, 98; Plyer, 2020). The implementation of cyber crisis communication plans for cyber-attacks can provide the necessary information relating to the nature of cyber-attack, risk assessments and cyber defenses for effective decision making (Plyer, 2020), e.g. the organisation's objectives in tackling cyberfraud, actions that the clients, management and employee must take to mitigate the occurrence of cyberfraud, the tools required for the implementation of the course of actions, the nature of cyberfraud with the response level, advices that can ease the concerns and questions of clients or stakeholders, responsible staff and the contact information. As part of the communication plan, cyber security alert can be initiated to sensitise the employees, clients and other stakeholders on cyber risk as well as information on how to update systems and mobile devices (Plyer, 2020).

Next is the alignment of the actions plans with the organisation's objectives. Better alignment between the risk management processes (identification, measurement, evaluation, mitigation and monitoring of

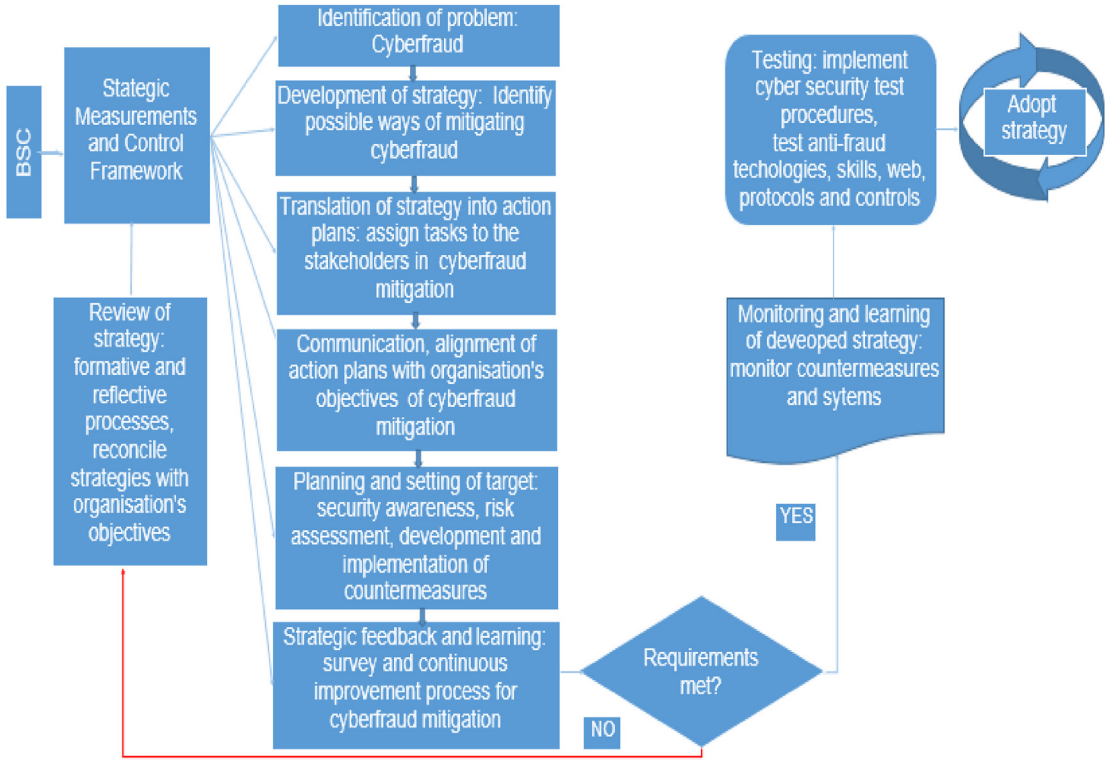

Figure 3. The process flow diagram for the strategic measurements and control for cyberfraud mitigation. Source: Authors' synthesis, derived from Niven (2006).

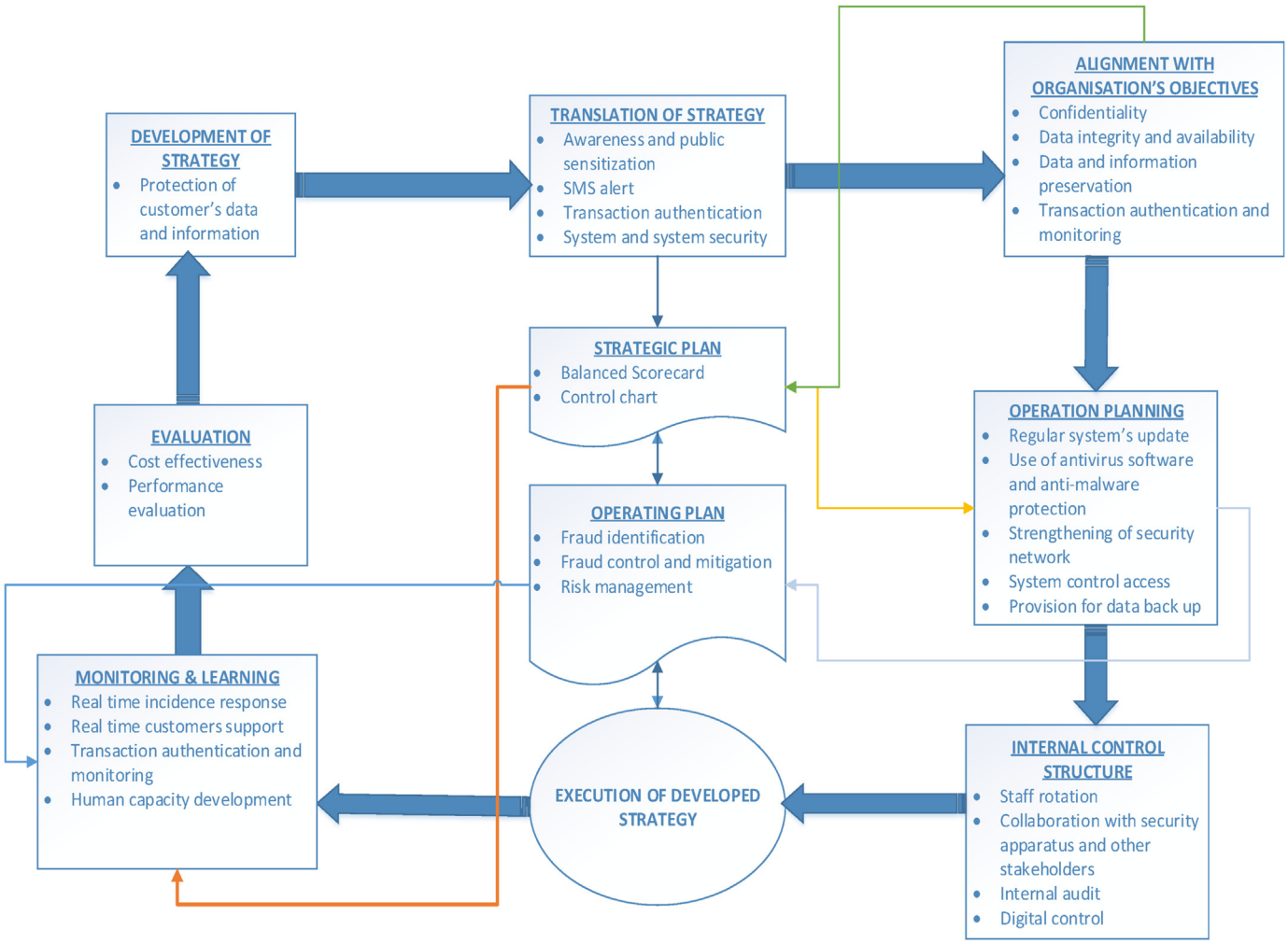

Figure 4. BSC perspectives for strategic management (measurement and control) system for the banking sector. Source: Authors' synthesis, derived from Niven (2006).

the risks) and the organisation's strategy is necessary for fraud prevention (Joel and Vyas-Doorgapersad, 2019:17). In line with cyberfraud mitigation, Primer (2016:38–44) explains that the development of cyber security plans will direct an organisation towards the prevention and mitigation of cyberfraud and its impacts. It will provide an effective means to reduce the litigation and insurance costs and sets out security policies as well procedures and countermeasures. This will ensure the integrity of operation and safety of cyber infrastructure. According to Primer (2016:40) cyber security planning can be achieved in four phases namely: security plan awareness (phase 1), assessing the risks of the physical as well as the online components to identify vulnerability (phase 2), security plan and countermeasures development (phase 3) and implementation of security measures including maintenance plan (phase 4).

Finally, a system of monitoring, control and innovation is necessary before the adoption of the BSC strategy for cyberfraud mitigation. The process of monitoring and assessing security efforts is crucial to the overall success of cyberfraud mitigation and will provide confidence about the capability of the security controls to mitigate cyberfraud risks (Lebanidze, 2011:17f). Monitoring and control of communications of the information systems (both internally and externally) to detect and prevent malicious intrusions and other unauthorized communications can be achieved via the use of protection devices such as gateways, proxies, routers, firewalls, and encryptions etc (Lebanidze, 2011:113).

If the requirements for effective mitigation of cyberfraud are met, the solution can be tested and deployed, otherwise, the proposed strategies can be reviewed. According to Lebanidze (2011:27), the testing phase is aimed at demonstrating the effectiveness of the control measures in mitigating cyberfraud risk. Hence, it is important for organisations to develop and implement standard cyber security test procedures. This may include testing of personal and client's awareness, testing of employees' skills and capability in the use of cyberfraud countermeasures, testing of access control and logging, testing of anti-fraud technologies and software, testing of web applications and protocols, testing of hosts and networks.

The next step would be a review process to reconcile the performance of the countermeasure deployed vis-à-vis the organisation cyberfraud mitigation objectives. Every process undertaken to mitigate cyberfraud will be assessed to identify and address inefficiencies capable of wasting resources and adding cost. This will assist the organisation ascertain whether the right cyberfraud mitigation solutions have been deployed. The outcome could lead to the reformulation of objectives, strategies and policies and/or affect the planning, execution and implementation of cyberfraud mitigation solutions. In the end processes which add value to the goal of cyberfraud mitigation will be retained and improved while non-value adding processes can be eliminated. Amongst others, the following should be reviewed to ensure alignment with organisation's culture, strategic objectives and resources in the effort to mitigate cyberfraud.

- Protection of customers' information and organisation's sensitive information.

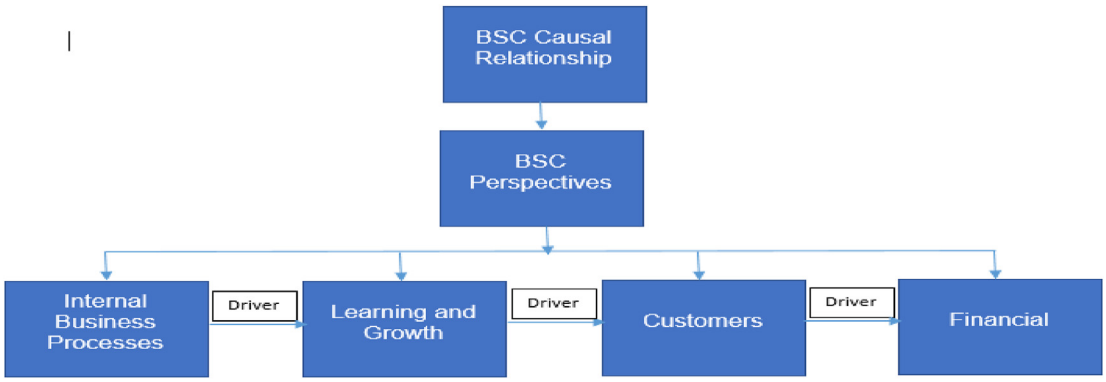

Figure 5. BSC causal relationship. Source: Derived and modified from Kaplan and Norton (1996b: 31)

- System to alert customers in any event of intrusion or cyberfraud in a timely manner.
- Consideration of the human factor including susceptibility to potential deviations from protocols or policy, either deliberately or due to ignorance.
- Training to develop employees' mindset on cyberfraud risk awareness in line with the organisation's short term goals and strategic vision.
- A clearly communicated risk management model for cyberfraud mitigation and business continuity as well as recovery plans in any event of cyberfraud.
- Inventory of information assests that must be safeguarded at all times.
- Policies relating to data breaches.
- Organisation's cybersecurity programmes or frameworks that are consistent with regulatory standards.

Table 2. BSC strategic measurement framework.

Strategic objectives	Strategic measurement (Lag indicators)	Strategic measurements (Lead indicators)
Financial • Improvement in returns • Broad revenue horizons • Reduction in cost structure due to cyberfraud related costs	Return on investment. Revenue growth Cost savings, reduction in the costs of the employed capacities of forensic accounting and of the management control system to minimise cyberfraud.	Revenue mix
Customer • Improvement in customer satisfaction • Protection of customers' data and information • Real time response to customers' distress call to halt cyberfraud • Improvement in customers' sensitization and awareness	Reduction in the cases of cyberfraud Implementation and effectiveness of security measures and anti-fraud technologies Increase in the number of aborted cyberfraud cases. Improvement in the customers capacities to protect themselves, reduction in the number of distress calls	Satisfaction survey Depth of interpersonal relationship Customers' feedback
Internal Business Processes • Mitigation of internal fraud risk • Effective responsive services • Strengthening of security network	Implementation and effectiveness of staff rotation, audit, and digital control measures	Robust internal control Effective alignment of personal goals
Learning and Growth • Strategic skills development • Provision of strategic information • Personal goals alignment	Human capacity development and employees' satisfaction Improvement in employees' capabilities	Strategic information and job coverage

Source: Authors' synthesis

- Effectiveness of the internal control measures.
- Cyberfraud risk-based investigation and incidence response schemes.

The internal control objectives may include the following:

- Protection of organisation's value. This includes the protection of the core organisation's work and ethical values as well as integrity.
- Protection of organisation's information.
- Risk management: This includes the identification of risk management objectives including the probability for cyberfraud and other internal or external factors that can affect the internal control structure.
- Activities control. This includes the control of all operational procedures and policies aimed at achieving effective operations and the risk management objectives.
- Information and communication control. This is necessary to implement various internal control measures and to ensure a balanced reporting following cyberfraud occurrences.

On this basis, the BSC perspectives can provide the management of the organisation with a detailed framework which translates a strategic cybercrime mitigation goal of the organisation into a set of performance

Table 3. BSC strategic control framework.

Phases	Actions
Problem identification	Establishment of the root cause-effect and forms of cyberfraud including the perpetrators
Development of strategy	Establishment of possible cost-effective ways of mitigating cyberfraud
Translation of strategy into action plans	Clarification of the vision of mitigating cyberfraud and ensuring that the strategies are interpreted into specific, measurable and realistic tasks
Communication and linking of action plans with objectives	Effective goal communication, education, training, public awareness and sensitisation about the nature of cyberfraud and countermeasures
Planning and setting of targets	Resource allocation, deployment of strategies, anti-fraud technologies, internal control, alignment of strategic initiatives and establishment of milestones. This can be achieved in four phases: 1. security plan awareness, 2. risk assessment, 3. security plan and development of response plans, and 4. implementation of adopted security strategies
Strategic feedback and learning	Strategic feedback, survey and continuous progress in the processes of learning and decision making as well as in the operation and implementation geared towards cyberfraud mitigation

Source: Authors' synthesis

measures. Figure 4 highlights the course of action necessary for mitigating cyberfraud in line with the four BSC perspectives.

As known from literature, the BSC can breaks down the organisation's vision and strategy into different objectives, measured in four perspectives: customer, financial, internal business process and innovation (learning and growth) (Kaplan and Norton, 1996b:30; Norreklit, 2000:67; Niven, 2005; Norreklit and Mitchell, 2007; Grigoroudis et al., 2010). The financial perspective recognises the performance of the organisation by its shareholders. With respect to cyberfraud mitigation, this relates to the cost effectiveness of the countermeasures, staff training, implementation of internal controls, as well as the potential costs savings in case the cyberfraud mitigation is indeed effective. In the same way, the customers' perspective relates to the safety of the customers in terms of data and information security, public sensitisation, and response to fraud incidences. Finally, with respect to cyberfraud mitigation the internal business process perspective could refer to strong internal controls, staff rotation, access control to the organisation's system, security and risk management training, modification of activities, business models, services and processes pathways. As usual, at the central of the four BSC perspectives is the translation of the organisation's strategy into action plans. Some of the action plans include awareness, public sensitisation, SMS alert, systems' security, transaction authentication and monitoring, confidentiality, and information preservation. The strategic plan, which involves the use of BSC, is linked to the operating plan for fraud identification, control, mitigation, and risk management. The strategic plan is also linked to each of the four BSC perspective as a bedrock for decision making.

Following Kaplan and Norton (1996a:4) as well as Norreklit (2000:68), who indicate that the BSC should encompass the performance drivers and outcome of measures, Figure 5 illustrates how the four perspectives are captured in a cause-and-effect relationship. This includes the operating plan for fraud identification, fraud risk control and mitigation as well as risk management (financial perspective), development of a strategy for the protection of customers' data and information (customers' perspective), internal control structure (internal business process perspective), monitoring and learning, development of human capacity (learning and growth perspective).

Looking at the original BSC, Kaplan and Norton (1996b: 31) assume the following causal relationships: the measures of organisation's learning and growth as a driver for the measures of internal business processes, while the measures of internal business processes act as a driver for the measures of the customer perspective and the measure of customer perspective as a driver for the financial measures. However, for the proposed model in this study, this causal relationship is slightly modified, seeing the internal business processes as drivers for the other three BSC perspectives (Figure 5).

To mitigate cyberfraud, some of the identified internal business processes include the development of strategies to achieve effective staff rotation, collaboration with security apparatus and other stakeholders, internal audit as well as digital control of the banking structures. The implementation of the developed internal business process strategies drives the learning and growth perspective. It deals with the development of human capacity to enable effective real time response to cyberfraud incidences, real time customers' support, transaction authentication and monitoring as well as deployment of anti-fraud technology to combat cyberfraud. By doing so, it drives the customers' perspectives which relates to the development and implementation of strategies to protect customers' data and information.

Table 4. The four perspectives of BSC and their respective measures for cyberfraud mitigation in financial institutions.

Perspectives	Tasks	Description	Possible performance measures
Financial	• Increase of shareholders value Reduction in revenue loss due to cyberfraud incidences	Covers traditional indicators such as growth, profitability and shareholder value.	• Return on the invested capital • Revenue growth • Earnings per share • Cash flow • Reduction in compensation cost for cyberfraud. • Reduction in the cost of loss in goodwill, shareholder value and infrastructure due to cyberattacks
Customer	• Addition of values to new and existing customers • Development of measures to promote safety of customers' information	Gives rise to customers' sensitisation, satisfaction and protection from cyberattacks. Also seeks the delivery of quality services.	• Inflow of new customers • Returns • Customer feedbacks or complaints • On-time service deliveries • Real time response to cyberfraud incidences and blockages • Reduction in the number of cyberfraud incidences.
Internal business processes	• Improvement of processes to achieve organisation's goals • Development of processes to check internal and external cyberfraud perpetration	Enhancement in the internal processes in addition to the decision making processes aimed at cyberfraud mitigation	• Services rejected • Speed of services • Information flow and management • Set-up time • Reduction in the number of cyberfraud incidences perpetrated both internally and externally • Proactive measures for blocking cyberfraud attempts • Processes for quick detection of cyberfraud
Learning and growth	• Implementation of continuous improvement processes and creation of future value • Frequent training and human capacity development in the area of digital and anti-fraud technologies	Aims at innovation, continuous improvement and creation of future value. Also aims at keeping employees abreast on the dynamics of fraud perpetration and use of anti-fraud technologies.	• Labour turnover rate • Income generated by new services rendered • Average time taken for service delivery • Improvement rates on other performance measures • Effective use of anti-fraud technologies for combating cyberfraud

Source: Own synthesis derived from Kaplan and Norton (2006:143–162).

Finally, the financial perspective is driven by the customers' perspectives in alignment with the organisation's objectives. The BSC strategic measurement and control frameworks are presented in Tables 2 and 3 respectively.

Table 4 presents the BSC perspectives in relation cyberfraud mitigation in financial institutions.

5. Conclusion and policy implications

The purpose of this paper was to develop a BSC strategic management control framework for mitigating the effect of cyberfraud. This was achieved using a qualitative approach involving the use of a structured questionnaire completed by the staff of 17 licensed banks in South Africa responsible for operations, management, and administration to capture their opinions with respect to the four BSC perspectives. One of the limitations of the qualitative approach employed in this study is that it cannot quantify data or present the numerical values from the information gathered. However, the exploratory potential of this approach was harnessed to gain a proper understanding of cyberfraud from the experts' opinions. The analysis of the expert's opinion assisted in the development of a strategic management (measurement and control) framework for the banking sector in the quest to mitigate cyberfraud occurrences. Another limitation of the qualitative approach is that it is subject to respondents' bias. This limitation was addressed by framing constructive questions that are open-ended to guide the respondents' in providing a balanced answer without simply agreeing or disagreeing. Furthermore, direct questions were asked to avoid assumptions and bias opinions. In addition, comparative analysis of the respondents' opinion was carried out to ensure that the conclusion reached is a fair outcome of the respondents' opinions and the situation of cyberfraud in the South African banking sector.

The findings from the study indicate that the significant effort is put into the reduction of the effect of cyberfraud on the customers by the South African banking sector and the sector is investing in the development of human capacity to reduce cyberfraud. The South African banking sector focusses more on the non-financial than the financial measures. However, the effect of cyberfraud negatively impacts the banking sector's revenues. The implementation of the proposed BSC framework may help to promote cyberfraud reduction, improve management control systems, performance measurements, as well as customers' and shareholders' satisfaction.

Furthermore, there is a need for the banking sector to ensure the compatibility of the forensic accounting techniques employed to mitigate cyberfraud with the management control systems. To reach this target, a BSC strategic management and control framework has been developed that can aid the process of cyber fraud mitigation if adequately deployed. It can also be employed as a strategic tool to balance the financial and non-financial measures. Efforts should be put in place to improve the indices of the financial measures. Taking the framework elements into account, the banking sector should work on the reinforcement of internal controls to allow for easy gathering of intelligence reports, regular auditing, effective supervision and monitoring, forensic investigations, necessary staff shuffles and/or redeployments. In addition, anti-fraud programs and control could be implemented as part of a fraud risk management to ensure regulatory compliance. The creation of a centralised fraud database may be encouraged as well to facilitate easy access to people's identity in a national database system, thereby forming a basis for a fraud management system. Furthermore, financial institutions may strengthen its security and intelligence apparatus so that they are more proactive in their approach to cyberfraud instead of just being reactive.

Declarations

Author contribution statement

Oluwatoyin Esther Akinbowale; Heinz E. Klingelhöfer; Mulatu F. Zerihun: Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data; Wrote the paper.

Funding statement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Data availability statement

No data was used for the research described in the article.

Declaration of interest's statement

The authors declare no conflict of interest.

Additional information

No additional information is available for this paper.

References

Akinbowale, O.E., Klingelhöfer, H.E., Zerihun, M.F., 2020. Analysis of cyber-crime effects on the banking sector using balance score card: a Survey of Literature. J. Financ. Crime 27 (3), 945–958.

Banking Association of South Africa, (BASA), 2015. The Banking Association South Africa Submission on Transformation in the Financial Sector [Online]. https://static.pmg.org.za/170314BASA.pdf. (Accessed 22 June 2020).

Bankscope, 2018. Bankscope Internet Quick Guide. https://www.bankscope.bvdep.com. (Accessed 19 October 2020).

Betianu, L., Briciu, S., 2011. Balanced Scorecard-Sustainable Development Tool [Online] Available at: http://anale.feaa.uaic.ro/anale/resurse/2011SEctb2betianu.pdf. (Accessed 20 February 2021).

Bhasin, M.L., 2011. Corporate governance disclosure practices in India: an empirical study. Int. J. Contemp. Bus. Stud. 2 (4), 34–57.

Bhasin, M.L., 2016. The role of technology in combating bank frauds: perspectives and prospects. Ecoforum 2 (5), 200–212, 9.

Cassim, F., 2016. Addressing the growing spectre of cybercrime in Africa: evaluating measures adopted by South Africa and other regional role players. School of Law, University of South Africa. In: Based on a paper presented at the First International Conference of the South Asian Society of Criminology and Victimology (SASCV) at Jaipur, India from 15–17 January 2011, pp. 126–138.

Chenhall, R.H., Langfield, S.K., 2007. Multiple perspectives of performance measures. Eur. Manag. J. 25, 266–282.

Clayton, M.M., 2011. Investigative techniques. In: Golden, Thomas W., Skalak, Steven L., Clayton, Mona M., Jessica, S. (Eds.), A Guide to Forensic Accounting Investigation, second ed. John Wiley & Sons. Inc., US., Pill, NJ, pp. 271–281.

Coovadia, C., 2011. Banking Sector Overview [Online] Available at. http://www.epiccommunications.co.za/sites/epic/files/cascoovadia_1_0.pdf. (Accessed 1 August 2019).

Detica Limited, 2011. The Cost of Cybercrime. United Kingdom, pp. 1–32.

Drucker, P.F., 2007. The Customer Is the Foundation of a Business. The Practice of Management. Routledge, New York, p. 31, 31.

Dzomira, S., 2014. Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. Risk Govern. Control Financ. Mark. Inst. 4 (2), 16–26.

Fincham, J.E., 2008. Response rates and responsiveness for surveys, standards and the journal. Am. J. Pharmaceut. Educ. 72 (2), 1–3 article 3.

Georgiev, M., 2017. The role of the balanced scorecard as a tool of strategic management and control. J. Innov. Sustain. 3 (2), 31–63.

Grigoroudis, E., Orfanoudaki, E., Zopounidis, C., 2010. Strategic performance measurement in a healthcare organisation: a multiple criteria approach based on balanced scorecard. Omega 40, 104–119.

Hogget, J., Medlin, J., Edwards, L., Tilling, M., Hogg, E., 2012. Accounting, eighth ed. John Wiley and Sons Australia, Ltd.

Idolor, E.J., 2010. Bank frauds in Nigeria: underlying causes, effects and possible remedies. African Journal of Accounting, Econ. Finan. Banking Res. 6 (6), 62–80.

Institute of Internal Auditors, 2009. International Professional Practices Framework, Practice Guide: Internal Auditing and Fraud, pp. 1–42 [Online] Available at. https://www.academia.edu/36393289/IPPF_Practice_Guide_Internal_audItInG_and_Fraud. (Accessed 25 March 2021).

Jegede, A.E., 2014. Cyber fraud, global trade and youth crime burden: Nigerian experience. Afro. Asian J. Soc. Sci. (4), 1–21. Quarter IV.

Joel, C., Vyas-Doorgapersad, S., 2016. An analysis of risk management within the department of trade and industry. J. Contemp. Manag. 16, 357–375.

Kaplan, R.S., Norton, D.P., 1992. The balanced scorecard – measures that drive performance. Harv. Bus. Rev. 70 (1-2), 69–79.

Kaplan, R.S., Norton, D.P., 1996a. Linking the balanced scorecard to strategy. Calif. Manag. Rev. 39 (1), 53–79.

Kaplan, R.S., Norton, D.P., 1996b. Using the balanced scorecard as a strategic management system. Harv. Bus. Rev. 74 (1), 75–85.
Kaplan, R.S., Norton, D.P.(, 2001. The Strategic-Focused Organisation: How Balanced Scorecard Companies Thrive in the New Competitive Environment. Harvard Business School Press, Boston.
Kaplan, R.S., Norton, D.P., 2006. Alignment: Using the Balanced Scorecard to Create Corporate Synergies. Harvard Business School Press, Boston Massachusetts.
KPMG, 2011. Cyber Crime – A Growing Challenge for Governments, 8, pp. 1–24. (Accessed 1 August 2019) [Online] Available at KPMG_INTERNATIONAL_Issues_Monitor_Cyber.pdf.
Kshetri, N., 2019. Cybercrime and cybersecurity in Africa. J. Global Inf. Technol. Manag. 22 (2), 77–81.
Lebanidze, E., 2011. Guide to Developing a Cyber Security and Risk Mitigation Plan. National Rural Electric Cooperative Association, Arlington, pp. 1–125 [Online] Available at. https://www.cooperative.com/programs-services/bts/documents/guide-cybersecurity-mitigation-plan.pdf. (Accessed 28 May 2021).
Meephlam, P., 2017. Challenges in Internet Fraud Prosecution and Investigation in Thailand: the Perspective of Thai Police Officers. A Dissertation Submitted in Partial Fulfilment of Master of Science in Criminology and Criminal Justice. Durham University, pp. 1–100.
Mohajan, H.K., 2018. Qualitative research methodology in social sciences and related subjects. J. Econ. Develop. Environ. People 7 (1), 23–48.
Monni, S., Sultana, A., 2016. Investigating cyber bullying: pervasiveness, causes and socio-psychological impact on adolescent girls. J. Publ. Adm. Govern. 6 (4), 1–26.
Moyo, B., 2018. An Analysis of Competition, Efficiency and Soundness in the South African Banking Sector. Economic Research South Africa, pp. 1–29 [Online] Available at. https://www.econrsa.org/system/files/publications/working_papers/working_paper_747.pdf. (Accessed 20 October 2020).
Niven, P.R., 2002. Balanced Scorecard Step by Step Maximizing Performance and Maintaining Results. John Wiley & Sons, New York.
Niven, P.R., 2005. Balanced Scorecard Step-by-step for Government and Non-profit Agencies. Wiley, Hoboken. New Jersey.
Niven, P.R., 2006. Balanced Scorecard Step-by-step: Maximizing Performance and Maintaining Results. Wiley, Hoboken, New Jersey.
Norreklit, H., 2000. The balance on the balanced scorecard – a critical analysis of some of its assumptions. Manag. Account. Res. 11, 65–88.
Norreklit, H., Mitchell, F., 2007. The balanced scorecard. In: Hopper, T., Northcott, D., Scapens, R. (Eds.), Issues in Management Accounting, 3. Prentice-Hall, Harlow.
Okeshola, F.B., Adeta, A.K., 2013. The nature causes and consequences of cybercrime in tertiary institutions in Zaria-Kaduna State, Nigeria. Am. Int. J. Contemp. Res. 3 (9), 98–114.
Ospina, S., 2004. Qualitative research. In: Goethals, G., Sorenson, G., MacGregor, J. (Eds.), Encyclopedia of Leadership. SAGE, London, pp. 1279–1284.
Öztürk, E., Coskun, A., 2014. A strategic approach to performance management in bank's: the Balanced Scorecard. Account. Finance Res. 3 (3), 151–158.
Plier, K., 2020. Effective Communication Mitigates Risk in a Cybersecurity World [Online] Available at. https://www.forbes.com/sites/forbesagencycouncil/2020/01/21/effective-communication-mitigates-risk-in-a-cybersecurity-world/?sh=24e9a2483afb. (Accessed 27 May 2021).
Prabowo, H.Y., 2011. Building our defence against credit card fraud: a strategic view. J. Money Laund. Control 14 (4), 371–386.
Primer, A., 2016. Cybersecurity plans and strategies, establishing priorities, organizing roles and responsibilities. In: Protection of Transportation Infrastructure from Cyber Attacks. The National Academics Press, US, pp. 1–170.
PwC Report, 2016. Banking in Africa Matters – African Banking Survey. Global Fintech Report, pp. 1–100 [Online] Available at. www.pwc.org [Accessed: March 2021].
PwC Report, 2018. Global Economic Crime Survey: Pulling Fraud Out of the Shadows, pp. 1–30. Available at. www.pwc.org. (Accessed 5 January 2019). Accessed.
PwC Report, 2019. The Future of Banking: A South African Perspective [Online] Available at. www.pwc.ac.za. (Accessed 31 July 2021). Accessed.
PwC's Global Economic Crime Survey, 2020. Global Economic Crime and Fraud Survey, seventh ed., pp. 1–32 [Online] Available at. https://www.corruptionwatch.org.za/wp-content/uploads/2020/06/global-economic-crime-survey-20201.pdf. (Accessed 17 January 2020) Accessed.
Rafiq, M., Zhang, X.-P., Yuan, J., Naz, S., Maqbool, S., 2020. Impact of a balanced scorecard as a strategic management system tool to improve sustainable development: measuring the mediation of organizational performance through PLS-smart. Sustainability 12 (1365), 1–19.
Ramamoorti, S., Morrison, D., Koletar, J.W., 2014. Bringing freud to fraud. J. Foren. Investig. Account. 6 (1), 47–81.
Rezaee, Z., 2005. Causes, consequences, and deterrence of financial statement fraud. Crit. Perspect. Account. 16 (3), 277–298.
South African Banking Risk Information Centre (SABRIC), 2019. Digital Banking Crime Statistics [Online] Available at. https://www.sabric.co.za. (Accessed 2 February 2020).
South African Banking Risk Information Centre (SABRIC), 2020. Annual Crime Statistics [Online] Available at. https://www.sabric.co.za/media/20oouwbg/sabric-annual-crime-stats-2020.pdf. (Accessed 20 June 2022).
Stojkovski, V., Nenovsk, B., 2021. Balanced Scorecard model in the banking sector. Int. J. Sci. Res. 10 (3), 1627–1630.
Tiwari, S., Bhalla, A., Rawat, R., 2016. Cybercrime and security. Int. Adv. Res. Comput. Sci. Software Eng. 6 (4), 46–52.
Uma, M., Padmavathi, G., 2013. A Survey on various cyber-attacks and their classification. Int. J. Netw. Secur. 15 (1), 390–396.
Voelpel, S.C., Leibold, M., Eckhoff, R.A., 2006. The tyranny of the balanced scorecard in the innovation economy. J. Intellect. Cap. 7 (1), 43–60.
Whittemore, R., Chase, S.K., Mandle, C.L., 2001. Validity in qualitative research. Qual. Health Res. 11, 522–537.
Wilson, N., Mcclean, S., 1994. Questionnaire Design: A Practical Introduction. University of Ulster. Copies Available from: UCoSDA, Level Six. University House, University of Sheffield, Sheffield S10 2TN.
Wu, J.C.T., Tsai, H.T., Shih, M.H., Fu, H.H., 2010. Government performance evaluation using a balanced scorecard with a fuzzy linguistic scale. Serv. Industr. J. 30 (3), 449–462.
Yanga, C.-H., Lee, K.-C., 2020. Developing a strategy map for forensic accounting with fraud risk management: an integrated balanced scorecard-based decision model. Eval. Progr. Plann. 80 (101780), 1–10.
Zhang, Y., Li, L., 2009. Study on Balanced Scorecard of Commercial Bank in Performance Management System. Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, pp. 206–209. May 22-24, 2009.