THE INTEGRATION OF FORENSIC ACCOUNTING AND THE MANAGEMENT CONTROL SYSTEM AS TOOLS FOR COMBATING CYBERFRAUD

Oluwatoyin Esther Akinbowale, Tshwane University of Technology
Prof. Heinz Eckart Klingelhöfer, Tshwane University of Technology
Dr. Mulatu Fekadu Zerihun, Tshwane University of Technology

ABSTRACT

Introduction: *One of the major challenges confronting the development of any nation results from fraudulent practices among the citizens of the country. This is also true for the banking sector: business has become more complex with the recent developments in information and communication technology. This has also changed the nature of bank fraud and fraudulent practices.*

Objective: *This study investigates the integration of forensic accounting and the management control system as tools for combating cyberfraud. It is geared towards the minimisation of the cost of employed capacities for forensic and management control systems in order to mitigate cyberfraud. The study also explores the effect of integrating forensic accounting and management control systems on banks' reputation and the loss of revenue resulting from cyberfraud.*

Methodology: *The study develops a conceptual model to show the relationship between forensic accounting, the management control system and cyberfraud in the banking sector. A linear programming approach was employed to express the relationship amongst the variables considered in this study with a view to reduce cyberfraud, minimise cost and improve the reputation of banks. This resulted in the formulation of a model which gives an idea of the feasibility of combining the components of forensic accounting, the management control system and bank reputation in order to combat cyberfraud. It was validated using the genetic algorithm solver which resulted in an acceptable, a logical and feasible fitness value and penalty value.*

Findings: *The ease of convergence of the fitness and penalty values of the solutions indicates that the developed model is feasible and suitable for achieving the set objectives.*

Conclusion and Recommendation: *The study demonstrates the feasibility of integrating forensic accounting and management control as tools for combating cyberfraud. Hence, this study suggests that the banking sector should implement a control on fraud risk management to ensure reputation and regulatory compliance.*

Keywords: Forensic Accounting, Management Control Systems, Cyberfraud, Information Technology, Reputation.

INTRODUCTION

Globally, cyberfraud is the second most reported economic crime affecting organisations and close to half of the organisations surveyed believe that local law enforcement is not adequately resourced to investigate economic crime, leaving the responsibility for fighting crimes on organisations (PwC Global Economic Crime Survey, 2016:66). An increase in cyberfraud is directly proportional to the deployment of technology in the business area, that is, the growing use of technology-enabled business processes such as point of sale purchase, automated teller machine transactions, e-commerce, online sales

processes, electronic business communication (e-mail) and so on, have made cyberfraud a threat to a wide variety of business operations (PwC Global Economic Crime Survey, 2014:6).

Obviously, this is also true for the banking sector: As an important part of the global economy, traditionally the banking sector represents financial institutions that strengthen the national economy through fiscal and monetary policy formulation, credit facilities and interest rate frameworks (Rayaan et al., 2016:2). However, the banking business has become more complex with developments in the field of information and communication technology, changing the nature of bank fraud and fraudulent practices. For example, ABSA and Standard Bank clients have lost between R1 million and R2 million to internet banking or SIM swap fraud, hence, they want the banks to be held liable for fraudulent activity (BusinessTech, 2017:2). According to Deloitte India Banking Fraud Survey Report (Deloitte, 2015:6),

"*Common causes of frauds in banking include diversion and siphoning of funds, whereas fraudulent documentation and absence, or overvaluation of collaterals were the main reasons for fraud in retail banking*."

In addition, fraud usually results in situations where stakeholders lose their trust in the industry, thereby leading to a loss of credibility and a crisis of confidence amongst the public (Abdinasir, 2017:2).

Therefore, establishing the challenges of fraud confronted by commercial banks in Kenya and identifying the strategies that banks use to combat fraud, Wanemba (2010:6) discovered that the banking sector has been losing a lot of money through fraudulent activities, leading to a negative impact on their profitability. Bankers though still insist that real damage is on increased operational costs, a build-up of bad debt, erosion of customer confidence and a steep drop in revenues as they are forced to invest in new technology to protect customer information. However, Akelola (2012:267) observed that the management control systems of some banks are in jeopardy because of the high cost of financing and sustaining information communication technology facilities assigned to aid information security.

Hence, the Management Control System (MCS) indeed could be the right point to step in if one wants to combat cyberfraud. Encompassing management accounting (as the driver of many organisations' decision making and control approaches; Otley, 2016:50) and other controls such as personal or clan controls (Chenhall, 2003:142), it is broadly concerned with the attainment of goals and the implementation of strategies, while forensic accounting systematically deals with the loopholes with which the quality of the services rendered by an organisation can be depraved by both internal and external fraudsters or con artistes. Therefore, effective forensic investigation calls for quality control, hence, Hauser (2006:512) described quality control as a means by which a firm obtains a reasonable assurance that expresses expert opinion and reflects the observance of approved quality standards, relevant acts/decrees and the codes of professional ethics. Quality standards provide evidence to third parties that proper steps haves been taken to achieve a high level investigation (Magrath & Weld, 2002:53).

Although it appears that management accounting/management control systems and forensic accounting may be the right tools to combat cyberfraud, none of the studies mentioned above pays attention to the integration of both of them as a tool for combating cyberfraud. In particular, it is not clear whether such an integration may aid cost effectiveness and promote the reputation of banks. Anti-fraud control can reduce the likelihood and potential impact of fraud; no entity is immune to this threat. This further implies that fraud cannot be completely eliminated but rather reduced.

LITERATURE REVIEW

Forensic Accounting

Forensic Accounting entails the integration of accounting, auditing, criminology and law; it is interpreted as an independent investigation, which is performed in the interest of the company owners and other stakeholders (Dubinina et al., 2018:132). Hence, forensic accounting is a technique which connects the conventional accounting system to the legal framework capable of uncovering fraud and providing a litigation support for the prosecution of the culprits (Karwai, 2004; Clayton, 2006:295). Therefore, forensic accounting can aid the fight against financial crime via the identification and tracking of suspected fraud cases (Hibshi et al., 2011:81; Grubor et al., 2013:1). In the view of Howard & Sheetz (2006), it is the process of interpreting, summarising, and presenting complex financial issues in a concise, detailed, and factual manner for the purpose of uncovering fraud. The analysis, interpretation, summarisation, and the presentation of difficult financial related issues are essential features of forensic accounting (Bhasin, 2007:1005). It involves thorough investigation of suspected fraud cases in which evidence gathered are expected to strictly follow the rule of evidence to gain acceptance in the court of law. Forensic accountants are taught to always consider the investigation of the numbers involved in case alongside the business realities of the suspected criminal cases. In this study, forensic accounting is considered alongside fraud detection, fraud investigation, fraud prevention and network security for the purpose of mitigating cyberfraud.

As a special practice area of accounting, forensic accounting describes engagement resulting from actual or anticipated disputes or litigation. It is fast becoming popular in providing evidence in the prosecution of corruption and as well assists in dispute resolution (Okoye & Gbegi, 2013:12). To conduct a forensic computer investigation, the forensic accountant should size up the situation, log every detail, conduct an initial survey and assess the possibility of ongoing undesirable activity. Regarding the information technology and systems, the computers should be powered down and checked for booby traps. Before analyzing the hard drive, the forensic accountant should further duplicate the computer hard drive or other permanent storage unit.

Management Control Systems and their Importance

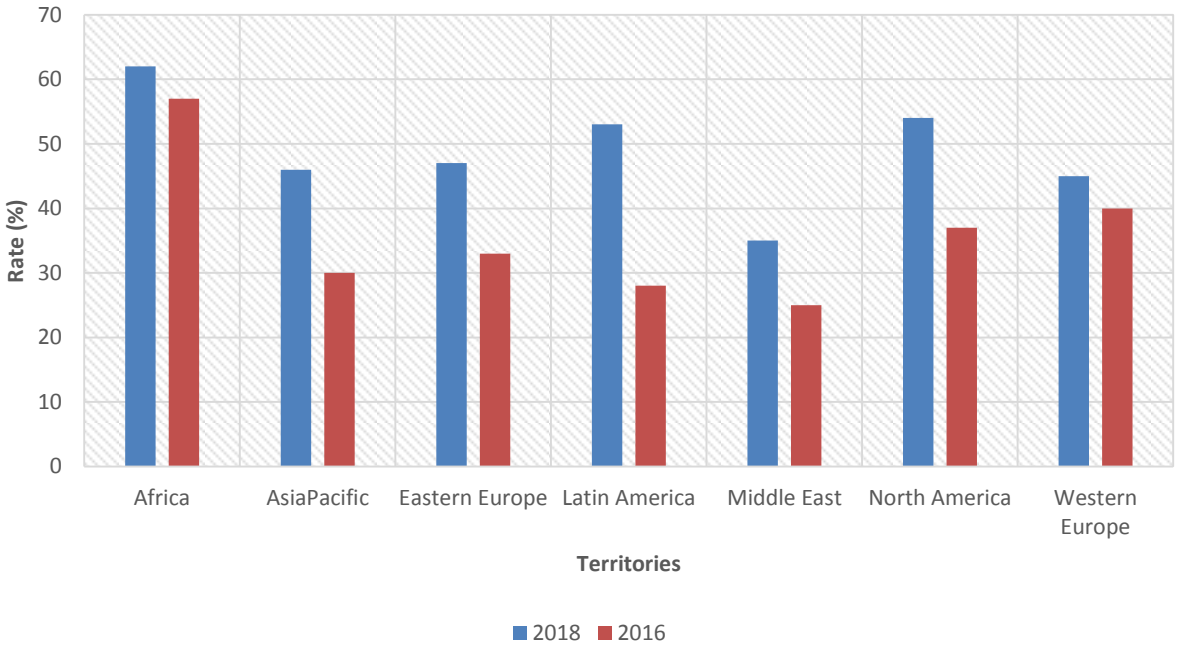
A Management Control System (MCS) as defined by Langfield-Smith (1997:215) is the process by which managers ensure that resources are obtained and used effectively and efficiently in the accomplishment of the organisation's objectives. In doing so, it has to monitor not only the internal environment, but must also be sensitive to external changes (Armesh et al., 2010:198). Therefore, information technology (IT) plays a central role in this process. Consisting of devices and systems that managers use to ensure that their employees' decisions and behaviour are consistent with the organisation´s strategies and objectives, it is an integrated system and needs to assess the organisation from every angle (Malmi & Brown, 2009:290). This means that controlling the organisation's behavior just from the accounting or managing view cannot fulfil the requirements of a comprehensive system.

Examining the relationship between strategy and non-financial performance measures in their study of the antecedents of management accounting change, Baines & Langfield-Smith (2003:690) revealed that a change towards a differentiation strategy led to an increased use and greater reliance on more formal controls. This opposed the outcome of Ittner, Larcker and Rajan (1997:246) who found that the adoption of an informal MCS (in their study: non-financial measures) increased with the extent to which a firm follows a prospector strategy. Besides this, already Chenhall (1997:82), interviewed and surveyed

manufacturing firms and their reliance on manufacturing performance measures (MPM) in order to evaluate managers' performance and moderate the relationship between total quality management (TQM) and organisational performance with focus on the Chief Executive Officers in 39 Australian manufacturing firms. Results from this study provided support for the proposition that enhanced performance would be associated with the interaction between well-developed TQM programmes and a reliance on manufacturing performance measures.

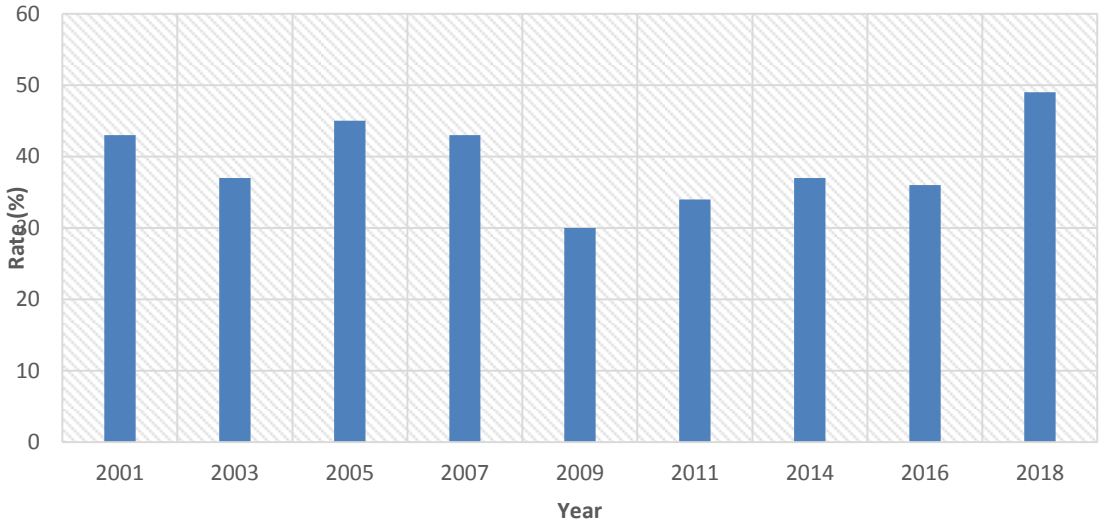
Existing Reports on Forensic Investigation and Economic Crime in the Banking Sector

In most banks, security measures are not taken with priorities and their approach can be quite lackadaisical (PwC Crime Survey, 2016:14). Investment in protection and detection is, therefore, meagre or non-existent. Such companies become easy prey for hackers. However, e.g. according to Ernst & Young (2016:10) cybercrime is perceived as the fastest growing fraud risk in India. In their survey, 40% of the respondents highlighted an increasing level of concern around cyber breaches or insider threats over the two years before 2016; 65% stated that these risks were leading to increased investment in Forensic Data Analytics (FDA). This shows companies' intent to have a more proactive approach and higher investment around cyber security going forward. In addition, PwC gave a comprehensive report on the economic crime rates across all territories for the year 2016 and 2018 as well as the global econmoic crime rates from 2011-2018 respectively. These reports are presented in Figures 1 and 2 respectively (PwC's Report on Economic Crime & Fraud Survey, 2018:3 & 7).



Source: PwC's Report on Economic Crime and Fraud Survey (2018:3)

Figure 1
ECONOMIC CRIME RATES FOR THE YEARS 2016 AND 2018



Source: PwC's Report on Economic Crime and Fraud Survey (2018:7)

Figure 2
THE REPORTED RATES OF ECONOMIC CRIME

With respect to the existing literature as well as the researchers' perspectives (Figure 3), it was observed that forensic accounting and management control systems are sets of related components that perform similar functions. The systemic nature of these variables describes the possibility of integration. The forensic accounting and management control systems have been identified as independent techniques which can aid the process of risk assessment and fraud management (Henderson & Greaves, 2011:320; Lueg & Knapik, 2016:78).

Of these, the risk assessment is an important phase of the risk management process because it is helpful in the determination of the extent that a potential threat and its inherent risk associated can impact an organisation (Stoneburner et al., 2002:8). This involves the identification, recognition, and evaluation of risk. On the other hand, the fraud risk management process comprises of fraud detection, prevention, and response. In an effort to analyse the effect of cyberfraud, Akinbowale et al. (2020a) reported on the use of four Balance Scorecard (BSC) perspectives namely the customers' perspective, the internal business processes, the financial perspective as well as the learning and growth perspective to determine the effect of cyberfraud in the banking sector. The results obtained indicated that the majority of the literature reviewed focussed on the effect of cyberfraud on the customers due to the fact that the customers are major determinants of the revenue level of an organisation. Akinbowale et al. (2020b) also reported on the development of two simplified models for tackling cybercrime. The first model addressed the incorporation of forensic accounting into the organisation's structure while the second one captured the detailed investigation and comprehensive data analysis processes of uncovering fraud.

During fraud risk assessment the incentives and motivation behind the fraud mitigation are unravelled. This is necessary in the development of control strategies to effectively mitigate fraud. After assessment, risk analysis and controls are necessary to determine the likelihood of a future adverse event and prevent its occurrence. In order to determine the likelihood of a future adverse event, threats to an IT system must be analysed alongside with the potential vulnerabilities and the controls in place for the IT system (Stoneburner et al., 2002:8). The novelty of this study lies in the fact that the development of a linear programming approach to express the relationship amongst the sub-variables of

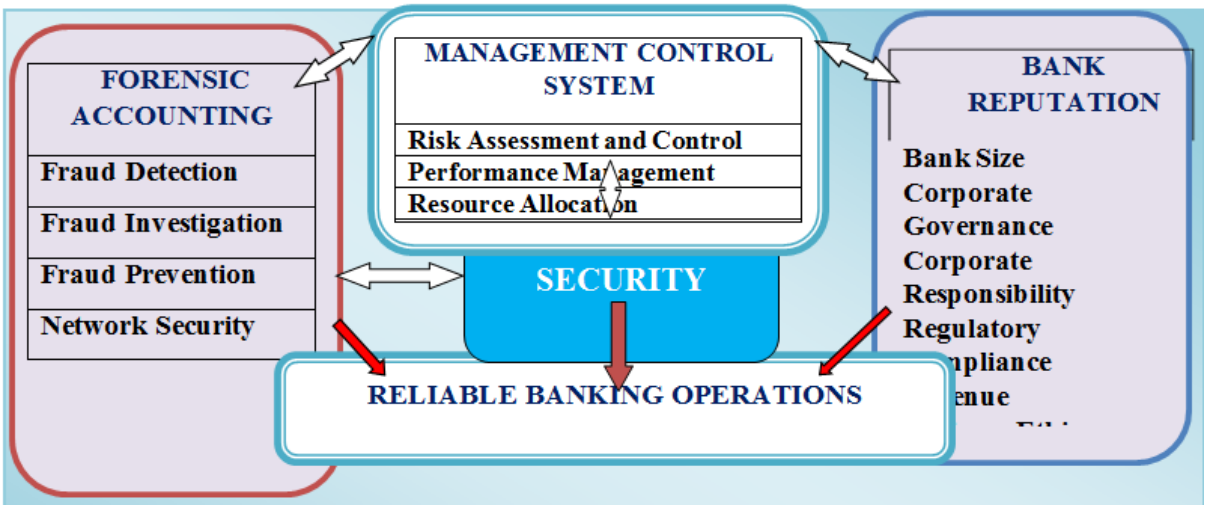
forensic accounting and the management control system with a view to reduce cyberfraud, minimise cost and improve the reputation of banks has not been highlighted by the existing literature. As the focal point, this study aims to give an idea of the feasibility of combining the components of forensic accounting, the management control system and bank reputation in order to combat cyberfraud.

METHODOLOGY

On the basis of the literature review, a conceptual model was developed, leading to a linear programming approach integrating forensic accounting and the management control system with cyberfraud and the bank´s repuation.

Conceptual Model

Obviously, reliable banking operations depend on several factors. With respect to the topic of this paper, the connections to forensic accounting, the management control system and the bank´s reputation seem to be worth to be further investigated and modelled (Figure 3).



Source: Authors

Figure 3
THE CONCEPTUAL MODEL ON THE INTEGRATION OF FORENSIC ACCOUNTING, THE MANAGEMENT CONTROL SYSTEM, AND THE BANK'S REPUATION

The conceptual framework consists of both the independent variables (forensic accounting and the management control systems) and dependent variables (cyber security) that were considered in this work. Several authors have reported on the capability of forensic accounting for fraud mitigation (Izedonmi & Mgbame, 2011; Brown, 2015; Cusack & Ahokov, 2016; Bassey 2018; Perduv et al., 2018; Liodorova & Fursova, 2018; Serhii et al., 2019). Similarly, effective management control systems can enhance an organisation's performance including fraud mitigation and information security (Tekavčič & Peljhan, 2003; Henri & Journealt, 2010; Carenys, 2012, Slavoljub et al., 2015; Mohammed & Knapkova, 2016). Since forensic accounting and management control systems can independently mitigate fraud and promote information security, this study seeks to explore the possibility of integrating the tasks of forensic accounting (fraud detection, fraud investigation, fraud prevention, and network security) and the management control systems (risk assessment and control, performance management, resource allocation and transaction monitoring) for promoting information security, as well as fraud mitigation and risk management.

In literature, cyber security (Tariq, 2018:11), an effective management control system (Shurafa & Mohamed, 2016:79), the effective implementation of forensic accounting (Abdulraham et al., 2020:150) and bank reputation (Fang, 2005:29; Thomson & Jain, 2006:48; Buckley & Nixon, 2009:30) have been identified as some of the factors critical to the overall suceess of a banking institution. Hence, reliable banking operations, management control systems, forensic accounting and the bank reputation while, on the other hand, one would still try to minimise the cost of the employed capabilities for forensic accounting and management control systems.

This could be formalised in a way that both the MCS as well as the forensic accounting should fulfil certain minimum standards (which one might formalise in the form of constraints), in particular to keep cyberfraud low. Of course, keeping in mind the profit targets of the bank, this should be done in a cost-effective way. In the end this means that one could formalise this part of the problem as a cost minimising problem under minimum standard contraints and capacity constrainst for the MCS and forensic accounting.

On the other hand, the bank´s reputation also has a big influence, not only on the reliability of banking operations, but as well with respect to the overall profit target. One can even go as far and say that it is axiomatic that reputation matters in banking (Buckley & Nixon, 2009:30); with other words: it should be managed and protected as it is one of the reasons for its existence. The need to preserve reputation should deter banks from opportunistic behaviour that will derive short term gains at the cost of losing reputation and future income (Fang, 2005:29). Thomson & Jain (2006:48) argue that to successfully attract depositors and investors and to maintain share price, banks need to maintain a reputation for good corporate governance and regulatory compliance. This means with respect to the topic of this paper that it makes sense to maximise the bank´s reputation. In the literature the major factors affecting reputation (reputation risk) in the banking sector are identified as: bank size, market competition, the degree of corporate responsibility pursed by the financial service provider, the level of security, ethics/integrity, and quality of product/services, among others (Dinc, 2000: 798; Fang, 2005:27, Thomson & Jain, 2006; Buckley & Nixon, 2009:32). With respect to cyberfraud, forensic accounting and the MCS, it seems reasonable that of this list the following factors should be formalised: the degree of corporate responsibility, the level of corporate responsibility and regulatory compliance, the level of (information) security, the loss of revenue and ethics/integrity. Of these,

1. the loss of revenue is already captured by the cost minimisation target as well as
2. regulatory compliance and the level of (information) security by the minimum standards to be fulfilled, while
3. the degree of corporate responsibility and ethics/integrity can be formalised as own objectives.

The sub variables of forenic accounting and the management control systems are the decision variables for the optimisation problem. The sub-variables of forensic accounting are represented by $x_{11} - x_{14}$ as stated in the conceptual model, i.e. x_{11} represents fraud detection, x_{12} fraud investigation, x_{13} fraud prevention, and x_{14} network security, while $x_{21} - x_{24}$ represent the sub-variables of the management control system, i.e., x_{21} denotes risk assessment and control, x_{22} performance management, x_{23} resource allocation and x_{24} transaction monitoring.

Hence, with the cost coefficients c_{ij} and the coefficients r_{hij} for the impact of the decision variables on the bank´s reputation (represented by the remaining targets to be maximised, i.e. h =1 for the corporate responsibility and h = 2 for ethics/integrity), one gets for the objective function of the linear programming approach:

$$min.F = \sum_{i=1}^{2}\sum_{j=1}^{4} c_{ij}x_{ij} - \sum_{h=1}^{2}\sum_{i=1}^{2}\sum_{j=1}^{4} r_{hij}x_{ij}$$
$$= c_{11}x_{11} + c_{12}x_{12} + c_{13}x_{13} + c_{14}x_{14} + c_{21}x_{21} + c_{22}x_{22} + c_{23}x_{23} + c_{24}x_{24}$$
$$- r_{111}x_{11} - r_{112}x_{12} - r_{113}x_{13} - r_{114}x_{14} - r_{121}x_{21} - r_{122}x_{22} - r_{123}x_{23}$$
$$- rr_{124}x_{24} - r_{211}x_{11} - r_{212}x_{12} - r_{213}x_{13} - r_{214}x_{14} - r_{221}x_{21} - r_{222}x_{22}$$
$$- r_{223}x_{23} - rr_{224}x_{24} \quad (1)$$

This means, that the objective is to minimise the costs of the employed capacities of forensic accounting and of the management control system in order to minimise cyberfraud and to maximise the corporate responsibility and ethics/integrity. This is subject to
- minimum standard constraints for

+ information security IS (2) (with the coefficients is_j),

$$is_1x_{11} + is_2x_{12} + is_3x_{13} + is_4x_{14} \geq IS \quad (2)$$

+ regulatory compliance RCF regading forensic accounting (3) (with the coefficients rcf_j),

$$rcf_1x_{11} + rcf_2x_{12} + rcf_3x_{13} + rcf_4x_{14} \geq RCF \quad (3)$$

+ regulatory compliance RCM regading the MCS (4) (with the coefficients rcm_j)

$$rcm_1x_{21} + rcm_2x_{22} + rcm_3x_{23} + rcm_4x_{24} \geq RCM \quad (4)$$

- capacity constraints for

+ resources RESF available for tackling cyberfraud by forensic accounting (5) (with the coefficients $resf_j$),

$$resf_1x_{11} + resf_2x_{12} + resf_3x_{13} + resf_4x_{14} \leq RESF \quad (5)$$

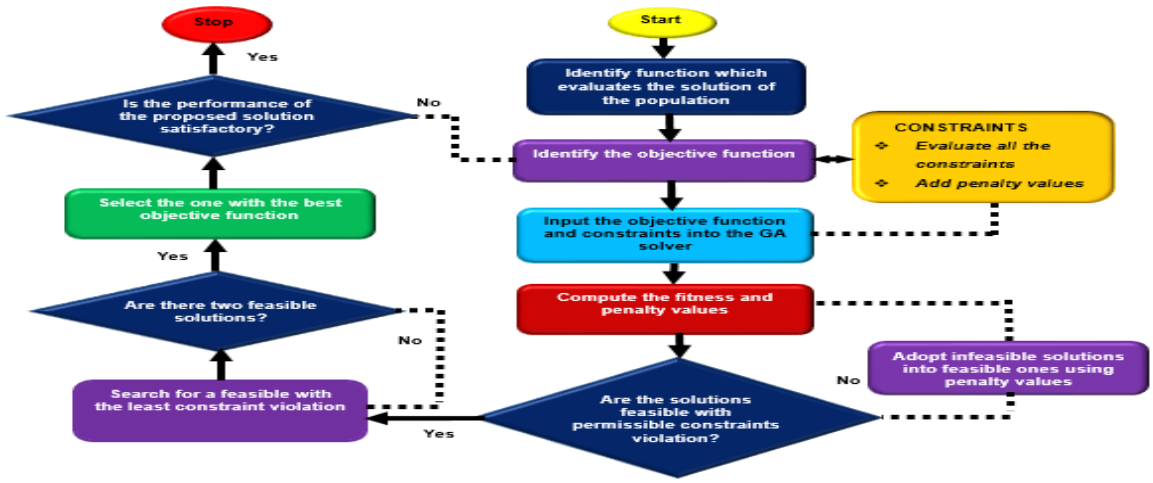
+ resources RESM available for tackling cyberfraud by the MSC (6) with the coefficients $resm_j$)

$$resm_1x_{21} + resm_2x_{22} + resm_3x_{23} + resm_4x_{24} \leq RESM \quad (6)$$

- non-negativity constraints

$$x_{ij} \geq 0 \quad \forall i \in \{1, 2\}, \quad \forall j \in \{1, 2, 3, 4\} \quad (7)$$

Model Validation



(Source: Authors)

Figure 4
THE FRAMEWORK FOR THE MODEL VALIDATION

To validate the developed model in order to determine the feasibility of the solutions and to justify the workability of the model, a Generic Algorithm (GA) was employed. The framework for the validation of the developed model is presented in Figure 4.

A GA solver is a stochastic, population-based algorithm for solving optimisation problems that searches randomly by mutation and crossover among population (Goldberg, 1989; Yeniay, 2005:45). The population of the possible solutions called the "*chromosomes*" evolves over succeeding generations with the aid of the genetic operators called "*reproduction*", "*crossover*" and "*mutual operators*" (Metawa et al., 2017:78). Barbozaa et al. (2015:563) explain that a GA is considered an efficient tool in generating optimal or near-optimal solutions to a variety of problems. Furthermore, it does not present some of the constraints associated with the traditional research methods. In addition, a GA is capable of finding a solution to problems that other optimisation strategies cannot resolve (Barbozaa et al., 2015:563). The merits of GAs as highlighted by Barbozaa et al. (2015:563) inform the decision of employing the GA for solving the developed linear programming model.

The fitness value, fitness (X_i) of an ith individual is expressed as equation (8) (Deep et al., 2009:508).

$$\text{fitness}(X_i) = \begin{cases} f(X_i), & \text{if } X_i \text{ feasible;} \\ f_{worst} + \sum_{j=1}^{m} \left| \varphi_j(X_i) \right|, & \text{otherwise;} \end{cases} \quad (8)$$

Where: f_{worst} is the fitness function of the worst feasible solution presently available in the population. The $\varphi_j(X_i)$ represent the values at the right hand side of the inequality constraints in equations 2-6 expressed as IS, RCF, RCM, RESF and RESM respectively.

For an infeasible solution, the fitness value is a function of the number of the violated constraints and the population of the solutions while the fitness of a feasible solution is the same as the value of the objective function. In a situation where there is no feasible solution within the population, f_{worst} will be set at zero (Deep et al., 2009:508).

As shown in Figure 4, the feasible solutions with no constraint violation or permissible constraints violation are always selected over the infeasible ones. The constraints are violated in the areas where the proposed solutions are not feasible. In a situation where there are two solutions are feasible, the solution with the best objective function would be selected. On the other hand, for two infeasible solutions, the one with the least constraint violation is usually selected (Deep et al., 2009:508).

The penalty function penalises the individual solutions which violate the constraints. To avoid constraints violation, infeasible solutions are adopted into feasible solutions by converting the optimisation problem into an unconstrained one using the penalty function.

The GA was employed to search for the optimum solution given the sub-variables of forensic accounting, and the management control systems.

The first step is the identification of a function which evaluates the solution of the population and indicates the objective function values. In the same function, the evaluation of all the constraints was done followed by the addition of penalty values which corresponds to the violated constraints in the objective function values. This gives the fitness value for the solution.

In order to do so, the objective function and constraints in the inequality form were given as input into the GA solver as a matrix with the specification of the decision variables. This was followed by the simulation in a MATLAB 2018b environment to obtain both the fitness and penalty values. The essence of the fitness value is to predict the suitability of the

objective function in achieving the set of goals while the penalty values determines the extent of violation of the constraints while achieving the goals.

RESULTS AND DISCUSSION

For the fitness value, the iteration terminated after 50 iterations out of 200 possible iterations after a feasible solution was reached. From Figure 5 one can see that the ease of convergence of the solutions after 50 iterations shows that the developed model is feasible and suitable for achieving the set objectives. The agreement between the best fitness value (3.0) and the mean fitness values (3.06) also indicates the suitability of the developed linear programming model in solving the problem.

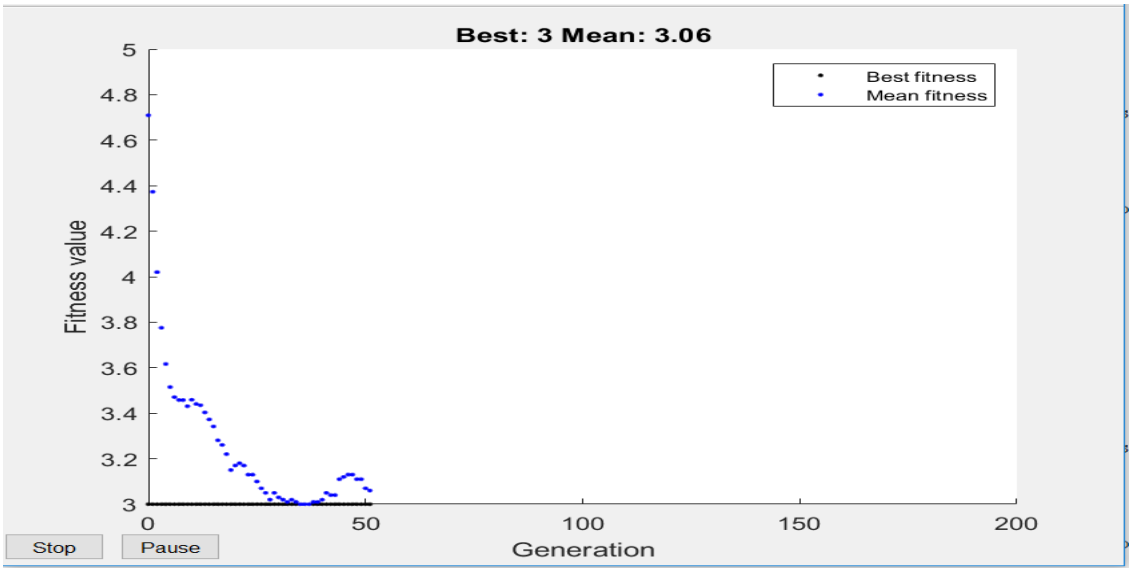


Figure 5
THE FITNESS VALUE

In addition, from Figure 6, the penalty value indicates non-zero where the constraints are violated and zero where the constraints are not violated. Most values of both the mean and the best penalty values converged at zero on the vertical axis, which indicates the closeness of the developed model to achieving the set of objectives without violating the constraints. The best penalty value was -2 while the mean penalty value was 78696.1. The wide difference between the best penalty value and the mean value indicates the non-violation of the constraints in achieving the set objectives. This implies that the proposed solution is feasible in achieving the objective function (i.e. to minimise the costs of the employed capacities of forensic accounting and of the management control system in order to minimise cyberfraud and to maximise the corporate responsibility and ethics/integrity).

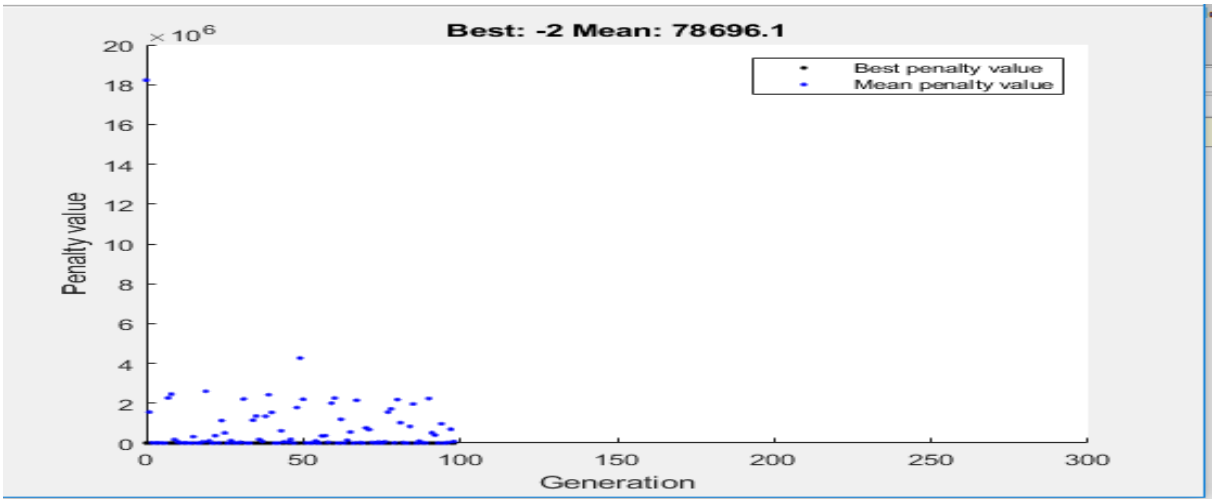


Figure 6
THE PENALTY VALUE

CONCLUSION AND RECOMMENDATIONS

Fraud is an intentional act of taking an individual's or a company's benefits illegally. Anti-fraud control can effectively reduce the likelihood and potential impact of fraud, the truth is that no entity is immune to this threat. This further implies that fraud cannot be completely eliminated but rather reduced. Basically, this study is focused on the integration of forensic accounting and the management control system geared towards the minimisation of cyberfraud. This resulted in the formulation of a mathematical model which gives an idea of the feasibility of combining components of forensic accounting, management control system and bank reputation in order to combat cyberfraud. The mathematical model was validated using a genetic algorithm solver which indicated the fitness value and the penalty value. The fitness value graph indicates an ease of convergence, which further implies that the linear programming model is logical and viable enough to achieve the set objective. On the other hand, the outcome of the penalty value graph indicates that there is no penalty because the constraints are not violated.

Therefore, the banking sector should ensure that the forensic accounting techniques employed to combat cyberfraud in their organisation are compatible with the management control systems introduced into the organisation.

REFERENCES

Abdinasir, G.A. (2017). The Impact of Forensic Audit services on Fraud detection among commercial banks in Kenya. A Research Project Submitted in Partial Fulfilment for the award of master's degree in Finance (MSC), School of Business, *University of Nairobi, 1-83.*

Akelola, S. (2012). Fraud in the Banking Industry: A Case Study of Kenya. Thesis submitted in partial fulfilment of the requirements for the Degree of Doctor of Philosophy, *Nottingham Trent University 1-422.*

Akinbowale, O.E., Klingelhöfer, H.E., & Zerihun, M.F. (2020a). Analysis of Cyber-Crime Effects on the Banking Sector Using Balance Score Card: A Survey of Literature, *Journal of Financial Crime, 27*(3), 945-958.

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.

Armesh, H., Salarzehi, H., & Kord, B. (2010). Management Control System. *Interdisciplinary Journal of Contemporary Research in Business, 2*(6), 193-206.

Baines, A., & Langfield-Smith, K. (2003). Antecedents to management accounting change: a structural equation approach. *Accounting Organisations and Society, 28,* 675-698.

Bassey, B.E. (2018). Effect of Forensic Accounting on the Management of Fraud In Microfinance Institutions in Cross River State. *IOSR Journal of Economics and Finance*, *9*(4), 79-89.

Bhasin, M. (2007). Forensic Accounting: A New Paradigm for Niche Consulting. The Chartered Accountant, *Country*, 1000-1010.

Brown, C.S.D. (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology, 9*(1), 55-119.

Buckley, R.P., & Nixon, J. 2009. The Role of Reputation in Banking. *Journal of Banking and Finance Law and Practice, 20*, 37-50.

BusinessTech, (2017). Major SA Banks taken to Court over Internet Fraud. [Online] Available at: https://businesstech.co.za/news/mobile/170629/major-sa-banks-taken-to-court-over-internet-fraud/, [Accessed: 1st August 2020].

Carenys, J. (2012). Management Control Systems: A Historical Perspective. *International Journal of Economy, Management and Social Sciences, 1*(1), 1-18.

Chenhall, R.H. (2003). Management control systems design within its organisational context: findings from contingency-based research and directions for the future. *Accounting Organisation and Society, 28,* 127-168.

Chenhall, R.H. (1997). Reliance on Manufacturing Performance Measures, Total Quality Management and Organisational Performance. *Management Accounting Research, 8*(2), 80-85.

Clayton, M.M. (2006). Investigative Techniques. In *A Guide to Forensic Accounting Investigation* edited by Golden, Thomas W., Skalak, Steven L., and Mona M. Clayton, Hoboken, NJ: John Wiley & Sons. Inc., US., 295-311.

Cusack, B., & Ahokov, T. (2016). Improving Forensic Software Tool Performance in Detecting Fraud for Financial Statements. In Valli, C. (Ed.). (2016). The Proceedings of 14th Australian Digital Forensics Conference, 5-6 December 2016, Edith Cowan University, Perth, *Australia*, 17-24.

Dada, S.O., Owolabi, S.A., & Okwu, A.T. (2013). Forensic Accounting a Panacea to Alleviation of Fraudulent Practices in Nigeria. *International of Journal of Business Management Economic Research*, *4*(5), 787-792, www.ijbmer.com | ISSN: 2229-6247.

Deloitte, (2015). India Banking Fraud Survey Report (Edition II), *pp. 1-36*, www.deloitte.com/in, access date: April 2018.

Dinc, S. (2000). Bank Reputation, Bank Commitment, and the Effects of Competition in Credit Markets. *The Review of Financial Studies*, *13*(3), 787-812.

Dubinina, M., Ksonzhyk, I., & Syrtseva, S. (2018). Forensic Accounting: The Essence and Prospects of Development in Ukraine. *Baltic Journal of Economic Studies, 4*(1), 131-138.

Ernst & Young, (2016). Forensic Outlook: Driving Ethical Business Growth in a Dynamic Risk Environment, 1-20, www.ey.com/in/FIDS, access date: November 2018.

Fang, L.H. (2005). Investment Bank Reputation and the Price and Quality of Underwriting Services, *The Journal of Finance*, *60*(6), 29-61.

Grubor, G., Ristić, N., & Simeunović, N. (2013). Integrated Forensic Accounting Investigative Process Model in Digital Environment. *International Journal of Scientific and Research Publications, 3*(12), 1-9.

Hauser, M.D. (2006). Moral minds: *How Nature Designed Our Universal Sense of Right and Wrong*, 1-520. New York, Harper Collins.

Henderson, W.M., & Greaves, P.J. (2011). Anonymous Communications. *In A Guide to Forensic Accounting Investigation, Second Edition* By Thomas W. Golden, Steven L. Skalak, Mona M. Clayton and Jessica S. Pill. PricewaterhouseCoopers, US., 313-330.

Henri, J.F., & Journealt, M.A. (2010). Eco-control: The Influence of MCS on Environmental and Economic Performance. *Accounting, Organisations and Society, 35*, 63-80.

Hibshi, H.A., Vidas, T., & Cranor, L. (2011). Usability of Forensics Tools: A User Study. 2011 Sixth International Conference on IT Security Incident Management and IT Forensics, Stuttgart, Germany. IEEE Computer Society, 81-91.

Howard, S., & Sheetz, M. (2006). *Forensic Accounting and Fraud Investigation for non-Experts*, New Jersey, John Wiley and Sons Inc.

Ittner, C.D., Larcker, D.F., & Rajan, M.V. (1997). The Choice of Performance Measures in Annual Bonus Contracts. *The Accounting Review*, *72*, 231-255.

Izedonmi, F.I., & Mgbame, C.O. (2011). Curbing Financial Frauds in Nigeria, A Case for Forensic Accounting. *African Journal of Humanities and Society, 1*(12), 52-56.

Karwai, M. (2004). Forensic Accounting and Fraud Investigation for Non-Expert, New Jersey: John Wiley and Sons, Inc., US.

Langfield-Smith, K. (1997). Management control systems and strategy: A critical review. *Accounting, Organisations and Society, 22*(2), 207-232.

Liodorova, J., & Fursova, V. (2018). Forensic Accounting in the World: Past and Present. *Journal of Economics and Management Research, 7*, 84-99.

Lueg, R., & Knapik, M. (2016). Risk Management with Management Control Systems: A Pragmatic Constructivist Perspective. *Corporate Ownership and Control, 13*(3), 72-81.

Malmi, T., & Brown, D.A. (2008). Management control systems as a package opportunities, challenges, and research directions. *Management Accounting Research, 19*(4), 287-300.

Magrath, L., & Weld, L. (2002). Abusive Earnings Management and Early Warning Signs. *The CPA Journal*, https://www.researchgate.net/publication/285201381, 48-55.

Mohammed, H.k., & Knapkova, A. (2016). The Impact of Total Risk Management on Company's Performance. *Procedia - Social and Behavioral Sciences,* 220, 271-277

Okoye, E.I., & Gbegi, D.O. (2013). Forensic accounting: A tool for fraud detection and Single prevention in the public sector: A study of selected ministries in Kogi State. *International Journal of Academy Research in Business and Social Sciences, 3*(3), 10- 23.

Otley, D.T. (2016). The contingency theory of management accounting and control: 1980-2014. *Management Accounting Research, 31*, 45-62.

Perduv, 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.

PwC. (2014). Global Economic Crime Survey 2014, *1-60, available at www.pwc.org, access date: July, 2018.*

PwC. (2016). Banking in Africa matters –African Banking Survey. Global Fintech Report, *1-100, available at www.pwc.org, access date: October, 2018.*

PwC. (2018). Global Economic Crime Survey: Pulling Fraud out of the Shadows, *1-30, available at www.pwc.org, access date: January, 2019.*

Rayaan, B., Samsudin, R.S., Che-Ahmed, A., & Popoola, O.M.J. (2016). The Moderating role of Capability Element of fraud on Internal Industry Factors and Fraud Prevention in Saudi Arabian Banking Sector. *International Conference on Accounting Studies (ICAS),* 1-9, Langkawi, Kedah, Malaysia.

Shurafa, R., & Mohamed, R.B. (2016). Management control system, organisational learning, and firm's performance: An Empirical Study from Developing Economy. *International Journal of Advanced and Applied Sciences, 3*(10), 79-88.

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.

Slavoljub, S., Srdjan, S., & Predrag, V. (2015). Management Control in Modern Organisations Faculty of Business Economics and Entrepreneurship. *International Review,* 3(4), 39-49.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk Management Guide for Information Technology Systems. *National Institute of Standards and Technology Special Publication, 800*(30), 1-53.

Tariq, N. (2018). Impact of Cyberattacks on Financial Institutions. *Journal of Internet Banking and Commerce, 23*(2), 1-11.

Tekavčič, M., & Peljhan, D. (2003). Insights into Managerial Tools Related to Cost Management in Slovenia Companies, Rijeka Faculty of Economics. *Journal of Economics and Business, 21*(1), 83-99.

Thomson, D., & Jain, A. (2006). Corporate Governance Failure and its Impact on National Australia Bank's Performance, *Journal of Business Case Studies, 2*(1), 41-50.

Wanemba, M.A. (2010). Strategies applied by commercial banks in Kenya to combat fraud. A Management Research Project Submitted in Partial Fulfilment of the Requirements for The Award of the Degree of Master of Business Administration, Department of Business Administration, School of Business, *University of Nairobi.*

Yeniay, Ö. (2005). Penalty Function Methods for Constrained Optimization with Genetic Algorithms. *Mathematical and Computational Applications, 10*(1), 45-56, 2005.