

## **The Effectiveness of Forensic Auditing in Detecting, Investigating, and Preventing Bank Frauds**

By

Kosmas Njanike, Thulani Dube and Edwin Mashayanye

### **Abstract**

*The study dwelt on the effectiveness of forensic auditing in detecting, investigating, and preventing bank frauds. The study sought to find out to what level the forensic auditors are able to fulfill this mandate and investigate problems that hinder forensic auditors to make progress in their operations in developing countries. It also established the role of forensic auditing in banking operations. Questionnaires, personal interviews, and document review are the methods that were used to obtain data for this study. A sample of thirty forensic auditors was used from thirteen commercial banks, four building societies, and four audit firms in Zimbabwe. It was found that the forensic auditing departments suffer from multiple challenges, amongst them being the lack of material resources, technical know how, interference from management, and unclear recognition of the profession. Types of bank fraud were identified. The internationally recognized audit procedures used in detecting and investigating these frauds were discussed. In conclusion, forensic auditors must be capacitated materially and technically to improve their effectiveness. In addition, the forensic auditors should create a constituted body that serves their interests and regulate the activities just like any other profession.*

**Keywords:** Bank fraud, Auditing, Detecting, Investigating, Preventing

## INTRODUCTION

Fraud together with its sister white-collar crimes which came into being later in the 19<sup>th</sup> and 20<sup>th</sup> century inter alia corruption, money laundering, tax evasion, externalization of foreign currency to itemize just a few have stood as potent weapons capable of hemorrhaging the entire world economies, particularly the banking sector because of its high risk factor. The susceptibility of the banking sector to fraud, from within and without, has not spared Zimbabwe (that registered a deep financial crisis in 2003/2004). Even the richest and electronically mobile countries have experienced a fair share of financial turbulence and uncertainties seeded by fraud-related crimes. The scandals sent shockwaves in the corporate world, regulatory authorities, audit fraternity, and the society at large; hence, the erosion of investor confidence in the financial markets (Levi, 2001).

The Zimbabwean banking sector has had a fair share of financial scandals. The Zimbank-Lorac financial impropriety (Goredema, 1992) and the reckoned 2003-2004 financial turmoil that saw the collapse of several banks due to deep-rooted mismanagement and poor corporate governance practices are a tip of the iceberg (Reserve Bank of Zimbabwe Report, 2006). Among possible causes of the collapse of Zimbabwean financial institutions were the shocking inadequacy of risk management systems and diversion of the core business to speculative activities contrary to the dictates of Sections 32 to 35 of the Banking Act (Chapter 24:20). High levels of non-performing insider loans, overstatement of capital adequacy (window dressing), and rapid expansion were some of the causes of the crisis (Reserve Bank of Zimbabwe Report, 2006). The financial malice saw the siphoning of more than one trillion Zimbabwe dollars into offshore accounts and the resultant escape of notable rogue bankers into hiding or self-imposed exile.

Although the Reserve Bank, as a regulatory authority, came in handy by appointing forensic auditors to investigate and determine the financial losses to the banks and clients and the resultant curatorship of the financial institutions, the damage had already been occasioned. Clients, potential investors, and the public have lost confidence and trust with the banking sector. The aftermath of the financial crisis evidenced the inexorable withdrawal of savings from the banking institutions by clients who had the worst belief and fear that their hard-earned cash would be swindled. The risk was evidently high among the new and emerging black-owned financial institutions.

Apart from the occupational frauds committed from within, the advent of new communication technologies has ushered in a plethora of other challenges, which emanate from without. Among the challenges are threats of computer fraud, cheque initiated frauds, identity frauds, credit card frauds, 'missing in the post' frauds, the use of fraudulent Real Time Gross Settlement (RTGS), and advance fee frauds, to name a few. The incidences of such frauds committed by outsiders in connivance with insiders have markedly compromised the security and risk of several banks.

It is within these challenges faced by banks that this research has been carried to determine the effectiveness of the forensic auditors whether outsourced or within in detecting, investigating, and preventing bank frauds. This study has also been prompted by the resultant economic malice ushered in by the unprecedented cases of fraud undermining the growth of the Zimbabwean banking sector. The role of forensic auditors has not been well articulated by several banking institutions, although some of them have created the posts in their organizations. The study seeks to explore forensic auditing techniques adopted by the banking fraternity and how they can be effectively used to assist the departments to achieve their objectives in detecting, investigating, and preventing bank frauds. Forensic auditing should be responsible for digging out frauds committed through application of auditing, accounting, and investigative techniques in order to come up with sufficient evidence that can be used in court proceedings (Albrecht et al, 2001).

### **Research Questions**

The paper thus strives to answer the following research questions:

- i) What are the different forms of bank frauds that need the attention of the forensic auditors?
- ii) What is the role of forensic auditing in banking operations?
- iii) Is the Zimbabwe banking environment conducive to forensic auditing?

### **CONCEPTUAL FRAMEWORK**

Forensic auditing is an activity that consists of gathering, verifying, processing, analyzing of, and reporting on data in order to obtain facts and evidence in a predefined context in the area of legal/financial disputes and/or irregularities and giving preventive advice (Institute of Forensic Auditors,

Belgium, 2004). Albrecht and Albrecht (2001) described forensic investigations as the utilization of specialized investigative skills in carrying out an enquiry conducted in such a manner that the outcome will have application to the court of law. Criminologists, just like their legal counterparts, have found it constantly challenging to define in its purest form and sample the constituents of fraud (Singleton et al., 2006). From a legal point of view, fraud situates itself as a generic term which embraces all multifarious means, which human ingenuity can devise, that are resorted to by one individual to get an advantage over another by false pretences (Nigerian Criminal Code, 1990). Levanti (2001) argues that no definite and invariable rule can be laid down as a general proposition in defining fraud. The United States Association of Fraud Examiners (1999), in a rather conservative fashion, identifies fraud as the fraudulent conversion and obtaining of money or property by false pretences: included are larcenies by bailee and bad cheque. The defunct Common Law Manual (Masango, 1998) argues that fraud is the unlawful making, with intent to defraud, a misrepresentation which causes actual prejudice or which is potentially prejudicial to another. It identifies essential elements as follows: unlawfulness, misrepresentation (which could be in the form of words, conduct, or failure to disclose); prejudice (which could either be actual or potential), and intention. What may be drawn as the common denominator for fraud is that the crime becomes into fruition where there is an element of misrepresentation.

Attempts to categorize fraud have been a daunting task to fraud specialists. One school of thought differentiates fraud according to occupation and non-occupational (Singleton et al, 2006) while another school serialized it on the basis of whether it is public or private sector fraud (Comer, 2001). However, another school accorded fraud in terms of industry in which the fraud was committed, such as bank fraud and insurance fraud (Skalah et al, 2001). Lendemen (2003) found it plausible to categorize fraud in terms of whether it is corporate or non-corporate, such as management fraud, insider dealing, investment fraud, and other related frauds. This study focused on the banking services industry.

Bank frauds have developed in nature and complexity from the traditional system of simple cheque fraud, where fraudster would just forge his name on a simple cheque by using an ordinary pen to more sophisticated techniques, such as the advance fee fraud which utilizes the Internet and computer highways (Singleton et al, 2006). Skalah et al (2001) managed to identify two species of fraud, those that are committed by insiders and those committed by other fraud felons outside. Among the bank

frauds emanating from within are: rogue traders, fraudulent loans, wire fraud, forged documents, theft of identity, and demand draft fraud. On the other hand, fraud committed by outsiders include: forgery and altered cheques, stolen cheques, cheque kitting, payment card fraud, booster cheque duplication and skimming of card information prime bank fraud, fictitious bank 'inspector' fraudulent loans applications, impersonation and theft of identity fraud and advance fee fraud, money laundering, and 'missing in the post' fraud.

According to Skalah et al, a rogue trader is a highly placed trader to invest sizeable funds on behalf of the bank. This trader makes risky investments using the bank's money, which when one investment goes bad, the trader engages in further market speculation in the hope of a quick profit which would hide or cover losses. Currency dealers usually commit some of the largest bank frauds (Singleton et al, 2001). Fraudulent loans are one way to remove money from a bank with practice bankers more than willing to encourage if they know that money will be repaid with interest (Skalah et al, 2005). The borrower may even be non-existent and the loan merely an artificial thing to conceal a theft of large sums of money from the bank (Hassibi, 2000). According to Skalah et al (2005), wire fraud makes use of wire transfer network, such as SWIFT, Real Time Gross Settlement (RTGS), and interbank fund transfer systems. While several banks have put some checks and balances in place, there is real risk that insiders may attempt to use fraudulently or forged documents, which claim to request a depositor's money, wired to another bank, often an offshore account in some distant foreign country (Skalah et al, 2005).

A discounting fraud is a confidence trick, where fraudsters use a company at their disposal to gain confidence with the bank, by appearing to be a genuine, profitable customer (Levi, 2001). After sometime, the bank is happy with the 'company' and the company may now request that the bank settle its balance with the company before billing the 'customer'. Levi argues that only when the outstanding balance between the bank and the company is sufficiently large, the 'company' takes the payment from the bank, and the company and its customer disappear, leaving no one to pay the bill issued by the bank.

A forged cheque fraud occurs where an employee issues a cheque without proper authorization (Skalah et al, 2005). Skalah et al argues that technique of altering information may be through use of chemical alterations, acetone, brake fluid, and bleach to remove or modify the handwriting. Instead of tampering with real cheque, some fraudsters will attempt to forge a depositor's signature on an unused cheque or

even print their own cheque drawn on an account owned by others, non-existent accounts, or even alleged accounts owned by non-existent depositors. The cheque will then be deposited to another bank and money withdrawn before the cheque can be returned as invalid or for non-sufficient funds (Hassibi, 2000). Stolen cheque books may be used by fraudsters who merely sign as if they were depositors (Skalah et al, 2005). Skalah et al stated that a booster cheque is a fraudulent or bad cheque used to make a payment to a credit card account in order to 'boost out or raise' the amount of available credit on otherwise legitimate credit cards. A stolen payment card can be used in fraud involving stealing the card itself and charging a number of high-ticket items to it in the first few minutes or hours before it is reported stolen (Hassibi, 2000).

Accounting fraud involves hiding serious financial problems, using fraudulent bookkeeping to overstate income, inflate the worth of the company assets or state a profit when the company is operating at a loss (Millichamp, 2002). This could be used to conceal theft in a company, as in the United States, the collapse of Enron and Tyco are cases in point (Skalah et al, 2005). Application, or skimming of information, is a fraud that takes a number of forms, ranging from dishonest merchant copying client card number for latter use to the tampered credit or debit card readers to copy the magnetic storage from a payment card while a hidden camera captures the number on the face of the card. The fraudulent equipment would then be removed and the data used to produce duplicate cards that could be used to make Automated Teller Machine (ATM) withdrawals from the victim's account (Hassibi, 2000).

Impersonation and theft of identity operates by determining information about the victim, then using that information to apply for an identity card, account, and credit card in the name of the victim (Hassibi, 2000). Cheque kitting involves the opening of accounts at two or more institutions and using 'float time' of available funds to create fraudulent balances (Hassibi, 2000). Hassibi argues that some perpetrators have swapped cheques between various banks on a daily basis, using each to cover the shortfall for the previous cheque. Fraudulent RTGS involves criminals who create counterfeit transfers purporting to be from a particular bank. They conduct business transactions with unsuspecting victims whom they engage as if genuine customers and pay the goods and services by use of these fraudulent RTGS (Puttick and Van Esch, 2003). Tricksters can use Automated Teller Machines (ATM), taking advantage of victims who are not able to operate an ATM. In Japan, the first manipulation of this facility started back in 1982 (Sieber, 1986). Advance fee fraud involves an upfront payment by a victim to the fraudster, to

allow the victim to take part in a much larger financial transaction, which he believes will bring him either profit or result in credit advanced to him (Smith et al, 1999). This fraud, because of its prevalence in West Africa, is also known as 419 scam, being a derivation from Section 419 of the Nigerian Criminal Code (Chapter 777 of 1990) which prohibits Advance Fee Fraud; Interpol, in the same vein, calls it “West Africa Fraud” (Smith et al, 1999).

Albrecht and Albrecht (2001) identified the following key functions of forensic auditing:

- To carry out the vision and mission of forensic audit to prevent, detect, and investigate issues of fraud and financial abuse within an organization/entity.
- Identification of causative factors and collection of facts for individual investigations by leading the evaluation of internal control weaknesses that allows unethical business behavior and practices to occur and go undetected.
- Lead internal/external resources in an effort to address allegations of fraud raised within the system.
- Provision of help in the development of fraud awareness training and analyze fraud trends and internal control procedures.
- Perform comprehensive analysis of investigations result across the enterprise to identify pervasive control issues.
- Oversee the investigations, planning, and forensic report writing process for forensic audits, and investigations and presentation of findings through reports and exhibits.
- Work closely with financial training function to enhance fraud-auditing skills.
- Develop the Fraud prevention, detection and investigation program and management of company’s Fraud Risk Assessment program.
- Conduct activities in areas of moderate to high risk.
- Conduct complex and extremely sensitive investigations.
- Promote education and awareness on fraud risk management throughout the bank.
- Testifying in court as an expert witness.

The forensic auditor should, if he were to succeed in his endeavor, have knowledge and understanding of fraudulent financial transactions, legal processes, high acumen of elements of fraud and criminological concepts, and above all investigative skills (Singleton et al, 2000). Levi (2001) concluded

that a forensic auditor is part cop, part lawyer, part accountant, and part psychologist. Van Horenbeech (2002) acknowledges that a forensic auditor should have a well developed professional skepticism ('sniffer' attitude and investigative mind), analytical and logical mind, personal integrity, expertise in internal controls, and acumen in interviewing techniques.

## **RESEARCH METHODOLOGY**

This paper used questionnaires, personal interviews, and document review to gather data. Data for the research was gathered from Forensic Auditors from thirteen commercial banks, four building societies, and four Audit Firms in Harare, Zimbabwe regardless of the time constraints they had. The research is a problem study designed to explore the relevance of forensic auditing in detecting, investigating, and preventing bank frauds. To generate an initial list of questionnaires designed to capture auditors' perceptions regarding bank frauds and how they manifest themselves, literature was reviewed extensively. The questionnaire consisted of three parts that is personal, detection, and investigations sections designed to capture information on the forensic auditing status quo and suggestions on the way forward. Three volunteer bank executives reviewed the questionnaire for readability, clarity, and completeness. Eighteen questionnaires with a cover letter explaining the purpose of the study attached were used for the study. Twelve personal interviews were conducted to afford greater exploration and time to probe and delve into the major emerging issues (Fowler, 1988; Easterby-Smith et al., 1995; Saunders et al., 2000). Ruyter and Scholl (1998) have indicated that, owing to the wealth of information that may be obtained from interviews, it is sufficient to hold only a small number.

### **4.1 Results**

## Profile of Respondents

Table 1 (below) shows the profile of the respondents where N=30.

**Table 1. Profile of Responding Forensic Auditors**

Academic and Professional Qualification	Frequency(n)	%
'O' Levels	30	100
'A' Levels	24	80
Professional Forensic Qualification	0	0
Other Banking Qualification(such as IOB)	12	40
Auditing Related Degree/Qualification	3	10
Orientation Courses	23	75
Police Background	24	80

All 30 respondents had at least passed their Ordinary Levels and joined their institutions having that qualification. A large majority (80%) of the respondents had passed their Advanced Levels and had commercial background. Only 10% had either an auditing related degree or qualifications. Few respondents (40%) had bank related qualifications, such as Institute of Bankers Certificate or Diploma (IOBZ), while none had a Master's Degree or any professional forensic qualification. Out of the total respondents, 75% indicated that they had undergone an orientation course in forensic auditing. It was discovered that 80% of the respondents were former police officers, particularly from the Criminal Investigations Department (Serious Frauds).

Data was sought on the length of service of each of the forensic auditors in the banking and forensic audit department. Half (50%) of the respondents were in the forensic department for less than five years, while 40% had worked for 5 to 10 years, with the rest having been in the system for more than 10 years.

## Types Of Bank Frauds

The various types of fraud that affected the Zimbabwean financial institutions (13 commercial banks) and the cost of such fraud to the economy were assessed. Table 2 shows the bank frauds identified, the number of banks affected, and overall economic costs of each type of fraud. The second column indicates the number of banks, and the last column of the table shows value prejudiced from 2006 to

2007 in Zimbabwean dollars. The results indicate that 5 (29%) out of 17 types of fraud affected all the financial institutions in Zimbabwe, that is cheque, identity, computer, accounting, and ATM fraud. Stolen payment card fraud and credit card fraud are occasioned in at least 5 of Zimbabwean banks, which represent 11%, whereas 3 (17.6%) of the banks each are affected by overdrawn fraud, application or skimming of information, and rogue fraud. Wire fraud, advance fee fraud, and bill discounting are not a threat to the banking sector in Zimbabwe.

**Table 2: Types of Fraud**

<b>Types of fraud</b>	<b>Number of banks</b>	<b>Value Z\$ (billion)</b>
Cheque Fraud	13	50
Identity Fraud	13	10
Credit Card Fraud	10	50
Stolen Payment Card Fraud	5	0.5
Credit Card Fraud	5	0.5
Computer Fraud	13	100
Fraudulent RTGs	13	50
Wire Fraud	Nil	Nil
Rogue Fraud	3	0.5
Bill Accounting	Nil	Nil
Accounting Fraud	13	100
Application/Skimming of Information	3	0.5
Cheque Kitting	10	5
Advance Fee fraud	Nil	Nil
Booster Cheque Fraud	8	5
ATM Fraud	13	50
Overdrawn Fraud	3	0.5
Paperhanging	Nil	Nil

### **Detection**

The detective approaches utilized by the forensic audit department were sought and 65% asserted that they use the proactive approach in the detective process, 25% employed the reactive approach, and 10% could use any. Enquiries were made to understand the detective techniques, which the forensic auditors employ in pursuit of their operational duties. It was discovered that out of the seven techniques available, the use of the surveillance equipment was popular, although not all banks were using it because of resource constraints to utilize them on a large scale. It was found that 60% of the respondents employ the Strategic Fraud Detection technique, whereas 40% have adopted the Risk-based profiling

technique. Of the respondents, 6 (20%) indicated that they engage the Red flag technique and all respondents avail the surveillance equipment method. On the availability of detection policy within the forensic audit department for effective discharging of duties, all have detection policies in their organizations which is usually combined with other elements of the risk management policy. The policy spelt out the responsibilities of the forensic auditor in countering any real or probable chances of fraud eventuating within the banking institution.

### **Investigation**

On the current investigative techniques in use by the forensic auditors and their effectiveness, 50% indicated that they used the forensic audit procedure, which is incorporated in the risk and control procedure manual of their organizations. The other half of the respondents pointed out that they do not follow any standard procedure as each case is treated on its merit. Nearly 60% of the respondents use both the forensic audit procedure and situational method when investigating. In order to determine the effectiveness of the forensic audit department on investigation of bank fraud attempted to measure it by collecting the total number of fraud cases received successfully completed and those in which they lost for the period 2006 to 2007. Data was obtained from 5 banks that offered to give information. In 2006, 720 cases were reported, of which 560 (78%) were completed successfully representing a clearance rate of 78%. On the other hand, 480 cases were reported in 2007 from January up to September 2007 and 300(70%) were successfully completed leaving a job in progress of 30%. The forensic auditors made use of different interviewing and interrogating techniques, which include the friendly method, you and me strategy, stress method, tell strategy, solution strategy, and the strategy mix. Findings from the 30 forensic auditors showed that 24 (80%) used the friendly strategy. Twenty-five used the stress method and sixty use the combination of friendly and tell strategy. The study sought to understand whether the forensic audit departments will operate with a constituted fraud investigations strategy, which may act as a guide or framework in their normal forensic auditing operations. It was discovered that 75 % had independent fraud investigations strategy, whereas 25% derived their strategy from the internal audit departments. On whether forensic auditors use a Fraud Risk Assessment as a way to preempt any potential fraud perpetrated by internal staff and outsiders, all indicated that they conduct it on different periods. Half of the respondents said they do so quarterly, while 25% perform it on half-yearly basis, and the rest on yearly basis. For fraud prevention measures, 49% used target-hardening approach, whilst 25% indicated their preference of the fraud prevention strategy, 29% used fraud control, and 10% used

the fraud control plan. The respondents were asked on the degree of management influence in conducting their business. About 75% asserted that they were independent from the influence of the top management when performing their daily duties except on issues that are strategic in nature, whilst 25% were partially independent as at times they are given unethical directives. The researcher enquired about the need to identify Forensic Auditing as a professional body responsible in regulating the activities of forensic auditors with professional codes of conduct, which every forensic auditor should adhere to like any other professional bodies. All indicated the need for creation of such a body that will protect the interests of forensic auditors and their reputation.

## **DISCUSSION**

There are at least thirteen types of fraud which are affecting the Zimbabwean banking sector. Among these, computer, accounting, RTGS, cheque and credit card frauds are prevalent in almost every banking institution accounting for 80% of the losses in banks. Computer fraud and accounting fraud pose a big challenge to the forensic auditor because of the complexity of the crimes, particularly where the computer software or system is manipulated. The Enron case, in which Jeffrey Skilling (then the Chief Operating Officer) and Kenneth Lay (the Chief Financial Officer) managed to misrepresent the status of the company's financial position through doctoring accounting information and on the other hand, the Arthur Anderson auditing gave a clean sheet of audit opinion on the status of the financial books (Albrecht et al, 2004). The collapse of banks in Zimbabwe was partly due to creative accounting, where banking institutions created two sets of books; one showing a healthy financial status and another a different picture altogether (Reserve Bank of Zimbabwe, 2006). The abuse of the computer was reflected by the recent National Merchant Bank criminal case, in which the bank was fleeced of 4.5 million in United States Dollars by Shame Mandara (The Herald, 2007). Although KPMG audit firm conducted two successive independent audits, they were not able to detect the fraud. This raised questions on the competency of the external auditors. In the American context, the failure of both the internal and external auditors gave birth to forensic auditing. However, the forensic auditors need to be articulate in information technology.

Generally, the detective approaches used by the forensic auditors included the proactive and the reactive. The use of each approach depended very much on the circumstances existing. Le (2001) reiterated that

the proactive approach is universally a tactical approach as it aggressively targets types of fraud, searches for their indicators, symptoms, or red flags. Preventive and detective techniques, such as the Five-Step Detection technique (Ernst and Young, 2006); Fraud Hypothesis Testing technique (Albrecht et al, 2004); the Strategic Fraud Detection technique (Albrecht and Albrecht, 2004); the Breakpoint technique (Hassibi, 2000), and the Bedford Digital Analysis technique (Nigrini, 1999) are generally proactive. They comply with the detective philosophy ‘we should catch fraud before it catches us’ (Comer, 2006). The reactive approach, which favors the philosophy, that; ‘we repulse when attacked or wait and see’ appeals to the use of electronic equipment, such as the closed circuit television (CCTV) or digital and mobile cameras.

The study showed that from the detective techniques, which are seldom used; include the Risk-profiling technique, the Peer-Group analysis, and the Digital Analysis technique. What may be drawn from the use of these techniques could be that the respondents are not familiar with the techniques. Some of them depend very much on accounting and computer proficiency, which the Forensic Auditor ought to have. Unlike in the developed world, most forensic auditing detective techniques are utilized. The Zimbabwean forensic auditors mostly depend on information fed to them through whistle-blowing and anonymous callers. Their core business is, therefore, to investigate cases handed over to them by bank departments and branches. The proactive approach to fraud detection is encouraged on the basis that it prevents the commission of fraud; ‘prevention is better than curing’. This is usually necessary for statutory investigations conducted on the now-defunct Royal Bank, Century Bank, Trust Bank, and Barbican Bank where financial misappropriations were unearthed. The use of modern detective techniques hitches on the information technology acumen and probing mind of the forensic auditor as most bank frauds are 80% computer initiated or that fraudsters use the computer as a conduit to defraud the bank (Albrecht and Albrecht, 2004).

Although all respondents claimed the possession of detection policies, they were in fact unwritten policies, by the overall risk management policies or fraud control policies. A fraud policy by nature is supposed to strategically guide the forensic auditor on detective approaches to bank fraud. All respondents asserted that the sources of the detection policies are the enabling legislation, such as the Banking Act, Building Societies Act, and the Post Office Savings Bank. The most debilitating handicap of most forensic auditors is that they do not have direct conduct with bank departments and branches so

that they can detect bank frauds. Where the forensic auditors are involved in the detection process, they tend to measure their effectiveness through a number of cases detected against potential and the resultant reduction. This yardstick does not take into consideration the likely impact of this possible reduction to increased confidence and trust among current and potential clients. In addition, the number of bank fraudsters arrested and convicted against potential will act as a tool of assessing the effectiveness of the forensic auditor. If there is high incidence of frauds, be it from within or without, clients, potential investors, and the regulatory authorities, particularly the Reserve Bank of Zimbabwe, lose confidence and trust which may result in the bank suffering irreparable damage.

It was observed that the investigative approaches used by the respondents vary from a one particular case to another. Some need standard forensic procedures, when others are situationally based and do not need specific standard procedures. The study discovered that half utilized the forensic audit procedures and the other half, acknowledged dependency on situational conditions. On scrutiny, it was discovered that what respondents call forensic audit procedure is fragmented and does not fully adhere to the internationally known forensic audit procedures as espoused by the American Institute of Certified Public Accountants (AICPA). The six points internationally recognized forensic audit procedure includes the following: public document review and background information, interview with knowledgeable persons, sending of confidential sources, laboratory analysis of physical and electronic surveillance, and undercover operations. In following this forensic audit procedure, there should be a link within the detection process so that synergy is built. The main duties of the investigator should be understood as securing, collecting, presenting, and considering the evidence on all sides of the issue, to be impartial and make findings and recommendations to the appropriate authority. Be that as it may, the forensic auditors move in this tumultuous line of operation, which advocate for situation investigations procedure.

Comer (2001) contends that a forensic auditor should think like a fraudster in order to work out possible methods of committing fraud. Every figure is significant, as it will lead and give a clue to the commission of a bank fraud. The investigator should be compelled to adopt a forensic attitude and assess the probable level and extent of complicity in the fraud within the organization. Then determine the knowledge, skills, and disciplines needed to effectively carry out the investigations, design audit

procedures in attempting to identify the perpetrator, extent of the fraud, techniques used, and coordinate activities with other stakeholders in the organization and the police.

In interviewing fraudsters and suspects, it was discovered that although there are at least seven techniques among them (namely friendly strategy, tell strategy, stress strategy, you and me strategy, and solution strategy) the most commonly used was the strategy mix. This could be because it appeals to different investigation situations, which they encounter. Where the suspect is cooperative, a 'friendly' and 'you and me' strategy will be suitable as it takes the interviewer and interviewee as equals. Where the suspect is uncooperative, then the stress and sustained strategies are ideal and evidence to prove a case beyond reasonable doubt should be gathered and synthesized. Evidence is said to be relevant if it could link the suspect to the fraud case committed, and material if its level of sufficiency could persuade the court to convict the accused.

Observations on the bank fraud cases received, successfully investigated, and those in which the forensic auditors were unable to account for the perpetrators, in monetary terms the success rate is not encouraging. The failure can be attributed to, among other reasons, the limited resources, technical know how, and management interference. Management interference manifests itself in their bid to play down fraudulent cases within the system and recommend de-activation of a case being investigated. Most indigenous banks that failed in 2004 had problems of this nature where certain dominant individuals within the system will fraudulently advance themselves loans and other illegal benefits at the detriment of the organization. It is important to note that those who report to another department, such as the internal audit, have generally limited avenues when investigating their cases. They do not have independent decisions to make in connection with some investigations. Where the internal audit department is falling short, the forensic auditors may not have the audacity to challenge them. Independence of the forensic auditors enables them to construct their strategies which fit into the way forensic audit procedures should be followed. All respondents conduct a Fraud Risk Assessment (FRA) to proactively pre-empt any potential fraud from both internal and external sources, although the frequency differed from one bank to another. The FRA is generally a tool used to counter any potential risks or threat that may affect the bank, chief among them being fraud. This assessment centers on the following aspects: identification of risk followed by identification of potential fraudsters, then possible

methods of fraud, the effectiveness of control, and possible concealment and possibilities of conversion (Ernst and Young, 2006).

The need for a concrete and well-communicated fraud control policy is important for the forensic auditor and the organization as a whole; the objective being to create awareness among staff and clients of the effects of bank frauds. In preventing fraud, most respondents used target-hardening method, Fraud Prevention Strategy, Fraud Control plan, and Fraud Prevention plan. However, there is not much difference in the use of these methods as they are modeled from a common Fraud Control Framework. The Australian Council of Arts developed a fraud control policy which every employee was party to. It included the following: policy statement, risk assessment, internal controls, internal reporting structures, external reporting structures, public interest disclosure, the investigation process, code of conduct, staff education and awareness, and client/community awareness (Crumbley, 2006). The forensic auditing department together with other responsible authorities should create adequate control systems to monitor compliance with established policies and procedures. Each member may be obliged to adhere to established codes of conduct, which sets the ethical values and norms of the financial institution.

The professionalism of forensic auditing and the departments is an important step in recognizing the value of the job. The profession in Zimbabwe needs to be recognized and regulated, as in the United States where forensic auditors are affiliated to the Association of Certified Fraud Examiners (AFCE). This may be done when and where there are standard qualifications for a forensic auditor. The essence of forensic auditing has not been well articulated within the organizational system let alone the banking sector. To some, the department stands as an impediment to their urge to enrich themselves while others believe that it is a management tool to safeguard bank assets through detecting, investigating, and preventing frauds within the system. Management and the board believe that the department is there in pursuance of organizational goals, which are survival and maximize shareholders' wealth. The forensic audit department is there to buttress the enterprise risk management process (Ernst and Young, 2006). It is important to identify and consider the skills and competences of forensic auditors and the level of academic qualifications of each individual. Nearly 80% of the respondents had police background, having worked in the Criminal Investigations Department (Serious Fraud Section). This pool of knowledge and experience, though ideal, is not sufficient for a standard forensic auditor. Most bank managements were of the opinion that the standard forensic auditor should possess the following

attributes: a background in accounting, banking experience, proficiency in information technology, an understanding of police operations, and being articulate with court procedures. According to the Association of Certified Fraud Examiners (USA), a standard forensic auditor should have at least an accounting degree, well versed in basic fraud theory, legal elements of fraud, criminology, interviewing techniques, proficient in the use of computer-based software, information analysis, and general internal control designs (Ryoba, 2005). This was confirmed by Van Herebeeck in Albrecht et al (2004) when he added that one should have a well developed professional skepticism ('sniffer' attitude and investigative mind), personal integrity, ability to see connection, follow through, analytical, logical, and a certification in auditing and investigation. In the Zimbabwean context, the whole sample adopted did not have any forensic related qualification to be recognized as such internationally. Except for 50% with professional qualifications, most of the forensic auditors lack that knack for figures and information theology, as their accounting background was mediocre. Those with a police background had an advantage on criminological issues and were better placed in interviewing techniques. The research found that most of the respondents are comfortable in using titles, such as 'security officer' or risk and control or investigations officer, other than forensic auditor. The reasons could be that 'forensic auditor' title limits their scope of job as some play a dual role of physical security and fraud investigations; hence, the core functions of the enterprise risk management. Others felt that the use of the title appeared foreign and flowery. However, more than 75% of the respondents had undergone in-service training that they enhanced their performance in the knowledge and skills needed. The in-service tends to motivate the subordinates within the banking system; hence, increase their effectiveness and productivity. It was discovered that experience had some bearing in performance and confidence in delivery of duty to forensic auditors in Zimbabwe as the saying that goes 'experience is the best teacher'.

## **CONCLUSIONS**

Forensic auditing, as an administrative function, has a role to play in the overall protection of bank assets. Forensic auditors have a mandate to detect any potential bank fraud and, if occasioned, conduct investigations of cases at hand and at least suggest effective ways of preventing the occurrence of such frauds. This can be effective where the environment is conducive for them to fulfill this mandate using available detective and investigative techniques to counter bank frauds.

Most forensic auditors have a police background whilst a few have a banking background. The forensic auditors are not professionally and academically qualified to investigate complex fraud cases. As experience is the best teacher, most bank frauds, which are not intricate, are successfully investigated and the accused are prosecuted. The majority of the forensic auditors is above five years in service and had undergone in-house training. Bank frauds vary from simple, easily detectable, and investigable to those, which are complex and difficult to detect and investigate. Those that are difficult to detect and investigate include those which are computer-related or which computer is used as a conduit to commit fraud. In Zimbabwe, at least thirteen types of fraud were discovered to be challenges in the banking institutions. Among these, five are dominant, which include cheque fraud, identity fraud, credit card fraud, computer fraud, and ATM fraud, which account for nearly 90% of bank losses.

Forensic auditors are not adequately equipped in terms of both materials, as has been reflected by the fact that they are not given a specific budget and usually fall under other departments. Most of the forensic auditing sections fall under either the internal audit department or the security department. This compromised their independence and professional integrity. The forensic audit departments seem to have fragmented forensic audit procedures that they follow. The forensic auditors generally do not understand the internationally recognized forensic audit procedures, only claim to follow the procedures, and only claim to follow the procedures as announced in the enabling legislation, such as the Banking Act (Chapter 24:20), the Building Societies Act (Chapter 24: 02), and Post Office Savings Bank Act. The detective and investigative techniques used by the forensic auditors include Strategic Fraud Detection technique, Risk-based profiling, red flag technique, and Surveillance equipment technique. For the purpose of effectiveness, the forensic auditor needs to use different techniques in detection, just like in investigation. The forensic audit department forms part of the overall risk management and, therefore, are party to the creating of the fraud control policy, which covers the detective, investigative, and preventive plans and strategies of the bank institutions. The study showed that the forensic auditing department suffered from multiple challenges amongst them being lack of material resources, technical expertise, interference from management, and clear recognition of the profession. Forensic auditing is still an emerging new profession, which needs to be developed.

## REFERENCES

- Albrecht, C. and Albrecht, U. (2004). Strategic Fraud Detection: A Technology-Based Model. Longman, New York.
- Albrecht, C. and Albrecht, U. (2001). Can Auditors Detect Fraud: A review of the Research Evidence: Journal of Forensic Accounting. Volume 11 pp.1-12.
- Association of Fraud Examiners Report. (1999).
- Bank, Uses, Promotion and Supervision of Money Laundering Act Chapter 24:24, Zimbabwe.
- Black, A. and Campbell, F. (1998). Black's Law Dictionary. Whaps Publishing. London.
- Comer, M. T. (2006). A Guide to Workplace Fraud and Criminal Behavior Recognition. [www.nao.gu.au](http://www.nao.gu.au) on 17/01/2008.
- Crumbley, D. L. (2001). Forensic Accounting: Older Than You Think. Journal of Forensic Accounting. Vol.1: 32-41.
- Ernst and Young. (2006). Fraud and Forensic Accounting and the Investigator. Kessler International Publication.
- Farid, B. and Franco, J. (1999). The Role of Auditor in the Prevention and Detection of Business Fraud. Butterworth. South Africa.
- Ferguson, G. A. (1981). Statistical Analysis in Psychology and Education. 5<sup>th</sup> Edition. McGrawhill Publishing.
- Front End Prevention of Financial Crime: Bankers Trust Company Security Service.
- Goredema, C. (2002). Collapse of Financial Services Sector. A Monograph. Juta South Africa.
- Gutman, P. (2000). Secure Detection of Data from Magnetic and Solid State Memory. University of Auckland. Auckland.
- Hassibi, D. (2000). Detecting Payment and Fraud with New Neural Network. Longman. Singapore.

- Krishna, S. S. and Lucas, D. M. (1978). Introduction in Modern Criminal Investigations. McGraw-Hill, India.
- Laurence, A. (1976). Practical Manual of Auditing. New Harper. New York.
- Leedy, P. D. (1985). Practical Research: Planning and Design. McMamillan Publication. New York.
- Leigh, A. (1982). Computer Fraud. Anderson. London.
- Lendemen, R. (2003). Implications for Investigations and Forensic Auditor. Boston Beacon Press. New York.
- Levanti, M. (2001). Prevention of Fraud. Crime Prevention Paper 17. London.
- Masango, C. (1998). Criminal Law Manual. Zimbabwe Republic Police Printers. Harare, Zimbabwe.
- Millichamp, A. (2002). Auditing. 8<sup>th</sup> Edition. Book Power. Johannesburg, RSA.
- Nigerian Criminal Code :Chapter 777 of 1990.
- Nigrini, M. (2006). Forensic Procedure and Spread: Useful Tools and Technique. downloaded from <http://antifraud.Aica.org> on 17/01/2008.
- Oaxley, H. (1989). The Principles of Public Relations: Kogan Page.
- Pany, K., Whittington, O.R., Mergs W. B. and Meirs, F. (1992). Principles of Auditing. IRWIN, Sydney.
- Puttick, G. and Van Esch, S. (2003). The Principles and Practice of Auditing. 8<sup>th</sup> Edition. Juta and Company Ltd.
- Reserve Bank of Zimbabwe Publications (2006). The Collapse of Barbican Bank: The Untold Story. Supplement to the First Half 2006.
- Reserve Bank of Zimbabwe Publications (2006). Monetary Policy Review Statement. July 2006.
- Ryoba, J. (2005). Importance of Building Forensic Audit Capacity in National Audit Office-Tanzania 2005-2006. National Paper. Tanzania.

Sieber, U. (1986). International Handbook on Computer Science. John Hopkins, New York.

Smith, A., Holmes, B. and Fauflan, D. (1999). Analysis of Advance Fee Fraud. Longman, London.

Singleton, J., Singleton, A. T. and Balogna, G. J. (2006). Fraud Auditing and Forensic Accounting.  
Mcgraw-Hill, London.

Skalah, S.L., Alois, M.A. and Sellar, G. (2005). Fraud: An Introduction. McGraw-Hill, London.

Silverstone, H. and Dawa, H. R. (2002). Fraud 101: Techniques and Strategies for Detection. John-  
Wiley and Sons, Ottawa.

Sproul, L.N. (1988). Handbook of Research Methods. Scarecrow Press. London.