BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

DEPARTMENT OF INTELLIGENCE AND SECURITY STUDIES

TOPIC

THE EFFECTIVENESS OF COMPUTERS IN FRAUD DETECTION AND PREVENTION A CASE OF ECOBANK ZIMBABWE BINDURA BRANCH

BY

THELMA SALATIELE

B1748969

A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE BACHELOR OF COMMERCE (HONOURS) DEGREE IN FINANCIAL INTELLIGENCE OF BINDURA UNIVERSITY OF SCIENCE EDUCATION, FACULTY OF COMMERCE.

JUNE 2021

APPROVAL FORM

The undersigned certify that they have supervised the student B1748969 dissertation entitled, 'The effectiveness of computers in fraud detection and prevention case of Ecobank Bindura', submitted in partial fulfilment of the requirements of the Bachelor of Commerce Honours Degree in Financial Intelligence.

…… **……/……/……**

Student **Date**

…… **……../……./…….**

Supervisor **Date**

…… **……./……./…….**

Chairperson **Date**

RELEASE FORM

Registration Number: B1748969

Dissertation Title: **The effectiveness of computers in fraud detection and prevention. A case of Ecobank Bindura**

Year granted: 2021

Permission is granted to Bindura University of Science Education Library and the department of Intelligence and Security studies to produce copies of this Dissertation in an effort it deems necessary for academic use only.

Signature of student.....

Date signed.....

DEDICATION

I dedicate this research project to all my family members who gave me all the support I needed throughout the academic period.

ABSTRACT

Banking business has become more complicated with development of information and communication technology which has changed the nature of fraudulent activities on Banks. The recent rise in cases of bank fraud in Zimbabwe has seriously reactivated a concerted debate of how effective computers are in the reduction of fraud. Therefore, this study sought to evaluate the effectiveness of computers, the factors affecting the effectiveness of computers and recommendations on improving effectiveness of computers in reducing bank fraud in Zimbabwe. The study covers a period of August 2019 to September 2020. A descriptive research design was used to gather data for the study. Questionnaires and personal interviews were used to collect data for the study. The data gathered was presented using tables, graphs and charts for easy interpretation and analysis. Ecobank Bindura branch was used as the case study for this research**.** The findings revealed that computers are effective in managing bank fraud as they detect and facilitate investigation and prosecution of fraud in the banking industry. However some factors were found to be affecting the effectiveness of computers these include poor internal controls, financial problems, and weakened societal values. The study concluded that the use of computers is not the sole solution for reducing fraud in the banking industry and therefore it recommended to improve internal controls, making use of bank reconciliations and also making use of whistle blowing as a mechanism to curb fraud.

ACKNOWLEDGEMENTS

Firstly I would like to acknowledge the presence, love and guidance of the Almighty God for he strengthened me. I would also like to extend my sincere gratitude to my entire family for emotional, moral and financial support. I would like to thank my supervisor for the assistance during the period I was doing my research project and also for the unwavering support and expert advice she gave me. I would also like to thank the Ecobank staff for responding and allowing me to carry out my research in their bank.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

1.0 Introduction

Fraud is an intentional deceptive action designed to provide the perpetrator with an unlawful gain or to deny a right to a victim. Fraud can occur in finance, real estate, investment, and insurance. It can be found in the sale of real property, such as land, personal property, such as art and collectibles, as well as intangible property, such as stocks and bonds. Types of fraud include tax fraud, credit card fraud, wire fraud, securities fraud, and bankruptcy fraud. Fraud can wear so many faces such as false insurance claims, pump & dump schemes, and identity theft leading to unauthorized purchases. Often, the perpetrator of fraud is aware of information that the intended victim is not, allowing the perpetrator to deceive the victim. Usually, the individual or company committing fraud is taking advantage of information asymmetry; specifically, that the resource cost of reviewing and verifying that information can be significant enough to create a disincentive to fully invest in fraud prevention.

1.1 Background of the study

Studies have shown that fraud is the biggest enemy of economies. Fraud exists in every economy and human effort. A glimpse of some headlines of daily newspapers reveals that fraud has caused the giant financial scams and scandals of a larger scale, a number of financial experts may agree that there is an inverse relationship between economic development and fraud .This study emanates on the backdrop of financial losses within businesses due to fraudulent acts and misrepresentations. As the business grows big it becomes more and more difficult to trace each and every cent within the company and it is from this background that fraudsters pounce and unjustly enrich themselves. Fraud has been found to negatively impact the overall aim of entities. Fraud shatters external confidence of the public as trust is lost when a company faces fraud allegations .Increased audit costs are also born out of fraud allegations as auditors will have to use a magnified eye into auditing

company books. When an auditor has to perform more procedures the audit cost increases. Fraud creates mistrust among workers and that has direct and indirect implications in the attainment of entity goals.

1.2 Problem Statement

In current times, fraud has been discovered to cause big threats to organizations. It is a big business risk which can incur a very big cost leading to a lot of problems of which one of them might be loss of confidence of shareholders and the public on the company. Fraud is a big business risk which if not prevented in the initial stage, it will have a very huge negative impact on organizational performance. The introduction of computers proves to be a way to solve the problem of fraud. This study seeks to determine the effectiveness of computers in reducing fraud.

1.3 Objectives of the Study

- To determine the effectiveness of computers in reducing fraud.
- To establish the role of computers in reducing fraud.
- To determine the factors which hinder or enhance the effectiveness of computers in reducing fraud.
- To determine the most precedent types of fraud in the banking sector.

1.4 Research Questions

- How effective are computers in reducing fraud at Ecobank?
- What is the role of computers in reducing fraud?
- Which factors hinder or enhance the effectiveness of computers in reducing fraud?
- What are the most precedent types of fraud in the banking sector?

1.5 Assumptions

- The questionnaires would be filled with relevant information needed by the researcher without any bias.
- Respondents had sufficient knowledge of the banking practice.
- Those respondents, who volunteered information, were truthful, co-operative and professional throughout the study.
- The data that the researcher gathered was accurate and reliable.
- The research was going to be carried out within the stipulated time as well as within the researcher's budget.

1.6 Significance of the Study

To the organisation

This study helps organisation to appreciate the role played by computers in fraud detection and prevention and gain knowledge on the different types of fraud. The study will help the organisation by shedding more light on the various fraud detection and prevention techniques that are computer based.

To the researcher

The research will enable the researcher to acquire increased level of knowledge in the area of study. The research will unleash a sense of academic development and achievement since it is partial fulfilment of undergraduate learning.

To the university

The research will add to the University's repository and will lay the ground for further studies by other students and members of staff, who may want to carry out research in related fields.

1.7 Delimitations of the Study

The study was focused on the effectiveness of computers in fraud detection and prevention in general. The research was limited to Ecobank Bindura branch which is part of the banking sector of Zimbabwe. As an introductory way the researcher explored a brief background of computers and a general appreciation of their impact on ease of doing business. This research looked at computer based fraud detection and prevention methods in a business environment. It covered the role of computers in fraud matters ever since they were invented to date mainly focusing on the period between 2020 and 2021 when the research was done.

1.8 Limitations

Lack of access to people was a major limitation to the study**.** The study depended on having access to people, organizations, data, or documents and due to the devastating effects of the COVID 19 pandemic access was sometimes denied or limited.Lack of cooperation from some members of the targeted population due to pressure from their daily routine duties. Unwillingness to cooperate negatively impacted this research. Some people were unwilling to provide information for several reasons others were eager to keep their operations a close secret. However as a researcher who needed the information I had to plead with them and convince them that the information was not going to be disclosed but rather kept confidential.

1.9 Organisation of the Study.

The research foundation will be as follows: First chapter involves introduction, background of the study, problem statement, objectives, research questions, significance of the study, assumptions, delimitation of the study and limitations. The second chapter looks at literature review which surveys books, scholarly articles, and other sources relevant to my particular topic. While chapter 3 will deal with research methodology and provide answers to questions such as how data was collected or generated? And, how was it analysed? The last chapter, Chapter 4, will cover the summary of the research, conclusion and recommendations.

CHAPTER II

LITERATURE REVIEW

2.0 Introduction

A literature review is a survey of scholarly sources on a specific topic. It provides an overview of current knowledge, allowing one to identify relevant theories, methodologies, and gaps in the existing research. This chapter critically looks at researches that have been done by others in relation to fraud. This chapter therefore focuses on conceptual framework, theoretical literature and empirical evidence.

2.1 Conceptual framework

2.1.1 Literature on the types of fraud

Asset misappropriation

The ACFE (1996) and ACFE (2002) described asset misappropriation as the misuse of employee's organization property including theft and payroll fraud. This type of fraud accounted for 80% of all the cases reported in the first edition of the ACFE report (ACFE, 1996) and 85% in the recent report (ACFE, 2014). Specifically, theft of cash, inventory and supplies are a common forms of assets misappropriation (ACFE, 1996, 2012). It is observed that asset misappropriation involving theft, fraudulent disbursement are the most frequent scheme type represented in the frauds reports (ACFE, 2012). Similarly, Price Waterhouse Coopers (PWC)'s Global Economic Crime Survey indicates that assets misappropriation accounted for 72% of the global crimes committed (PriceWaterhouseCoopers, 2014). However, it is observed that it has the least median cost when compared to other fraud schemes (ACFE, 2010, 2012). Having the highest frequency and lowest median cost, asset misappropriation is followed by corruption.

Corruption

Another occupational fraud scheme that attracted the attention of stakeholders is corruption. It is described by ACFE (2010) as the use of influence in a transaction in violation of duty for personal benefits. While the World Bank see it as the abuse of public office for personal gain (World Bank, 1997). It includes bribery, extortion and conflicts of interest (ACFE, 2012). Studies have linked corruption, especially in public sector, to economic development and social issues (Doig & Mclvor, 1999; Gupta, Davoodi, & Alonso-Terme, 2002; Mauro, 1995; Tanzi, 1998). This form of fraudulent scheme has been a major concern for policy makers and international organization (United Nations, 2004) and also subject of annual reports (Transparency International, 2014). In the ACFE annual reports to the nations, corruption accounted for 10% in 1996, 32% in 2004 and 36% in 2014, indicating a growing trends (ACFE, 1996, 2004, 2014). In addition, it is estimated that bribery alone accounts for over $ 1 trillion annually (Graycar & Sidebottom, 2012; Heineman & Heimann, 2006; Judge, McNatt, & Xu, 2011). While PWC found that corruption represented 27% of crimes in the 2011 crime survey (PriceWaterhouseCoopers, 2014). However, fraudulent statement has maintained the lead in corporate financial scandals (Soltani, 2014).

Fraudulent Statement

One of the current global challenges of the corporate world has been the issue of financial statement fraud (Rezaee, 2005). It is estimated to have caused investors more than $500 billion (Rezaee, 2005). A form of occupational fraud described as the falsification of an organization's financial statements and a deliberate Proceedings of the International Conference on Accounting Studies (ICAS) 2015 17-20 August 2015, Johor Bahru, Johor, Malaysia 503 attempt to deceive or mislead investors and creditors by materially misstated financial statements (ACFE, 2014; Rezaee, 2005). Specifically, involving overstating revenues and understating expense. The trend in fraudulent statement according to the ACFE annual reports indicates that it accounted for 5% in 2002 and with the median loss of $4,250,000 in 2002 (ACFE, 2002, 2004, 2012, 2014). The report has consistently found fraudulent statement to account for the least cases but having the highest median loss to organizations.

2.1.2 Literature on the role of computers

Forensic analytics software

Nowadays, there are many audit software that can assist auditors to improve the overall audit process and shorten the time to process it. Some of the software are namely; Audit Comand Language (ACL), Interactive Data Extraction and Analysis (IDEA), Statistical Analysis System (SAS), and Microsoft Data Analyser (Bagga & Singh, 2011, The ACL is one of the most leading tools in the industry and delivers audit data analytics to customers who want to oversee activities within their organizations. It is a tool that can assist auditors to test an enormous amount of data sets. The ACL can be used as audit data analytics, monitoring and auditing of the company, investigating and detecting fraudulent activities certifying compliance within company policies and developing secure data access for all users (Aiken, 2016). The auditors must inspect enormous quantities of data from a wide variety of computer platforms, while operating under severe time pressures. Companies and individuals must submit their tax data by electronic means, but they can do so in many formats. The ACL's flexible audit analytics software has been the key to the ability to enhance the scope and effectiveness of tax audits. In one major initiative, over a four-year period, the Electronic Data Processing (EDP) audit team has used powerful audit analytics to identify and then recover €85 million in missed tax revenues. The ACL gathers valuable information for decision-making purposes. The data will be checked manually to confirm whether all the required and adequate fields are provided or no The ACL is known for its processing data and handling large volume of data. Though the software itself is good, users need to pay large amount of money to acquire the license and also for the training session.

2.1.3 Factors which enhance the effectiveness of computers in fraud detection and prevention

An expert system can have a user-friendly interface that makes it easier to be used and it can perform real-time tests whether on historical data or new data. Not only that, it can be incorporated into a database and provide decision making based on the preference provided by the user. This is an advantage to detect fraud as the scenario can be changed to follow the current trend of fraud occurrence. Expert systems have the advantage of combining rules and profile extraction in the framework for fraud detection. These are considered good advantages for auditors since they can insert their own constraint to detect fraud. Besides its

user-friendly interface, it is also a reliable system that can be operated in real-time or on historical data. This option would enable auditors to compare latest result with prior results, thus they can keep their performance at the top.

Availability of Easy to get Free software (Microsoft Excel) for spreadsheets enhances the effectiveness of computers in fraud detection and prevention as bigger datasets can be manipulated and generate reports in the most minimal possible time.
The availability of computer networks aides the effectiveness of computers in the quest for fraud detection and prevention since it enables quick sharing of data and information across geographical boundaries. Computer technologies also provide for storage and backup of enormous data that can be used for references and comparisons

2.1.4 Factors hindering the effectiveness of computers in fraud detection and prevention

The downturn of computer applications in fraud detection and prevention is that it is difficult to transfer human expertise into the system due to miscommunication and different understanding of a certain topic. Comparing it to other tools, the spreadsheet tool is the least preferable tool because data might be changed inadvertently which will affect conclusive results. As for the forensic analytics software, despite being advantageous, the main problem with the software is the cost to obtain and for training. Big data technologies have security problems with their database because they are vulnerable to cyber-crime attack.

It is less expensive and more effective to prevent fraud from happening than to detect it after the occurrence this therefore means that fraud detection is expensive. Usually, by the time the fraud is discovered, the money is unrecoverable or the chance to recover the full amount of the loss is very slim. Furthermore, it is costly and time consuming to investigate frauds especially involving large-scale multinational operations. Therefore the large costs of detecting fraud hinder the effectiveness of computers in reducing fraud.

2.2 Theoretical review

2.2.1 The Theory of Fraud Detection and Prevention

This chapter provides an overview of traditional as well as new theories related to fraud. The key to prevent fraud is to understand that fraud exists and then limit its potential for harm. To do that, the detection of fraud is paramount, along with the exceptional fraud prevention

programs. Preventing fraud is often harder than it would appear. Human nature and greed guarantee that society and corporations would always face the issue of fraud. Lessening or removing the opportunity is one way to fight fraud. It can be accomplished by improved internal controls and accountability. Understanding the importance of fraud prevention is critical for a business organization in the new era of improved corporate governance. The Association of Certified Fraud Examiners (ACFE) is the world's premier provider of anti-fraud training and education. The ACFE's goal is to reduce business fraud worldwide and inspire public confidence in the value and integrity of the fraud detection and prevention profession. The ACFE also conducts studies and issues the reports on occupational fraud to examine the effects of occupational fraud and abuse on the individuals and organizations. The theory also provides a basis for understanding contemporary threats that are posed by new emerging forms of fraud and security measures and methods for preventing and controlling fraud. The theory is important to this study as it provides an understanding of the new methods and tools and being used by fraudsters.

Thanasak (2013) states that before making any efforts to reduce fraud and manage the risks proactively, it is important for the business organizations to identify the factors leading to fraudulent behaviour by understanding who are the fraudsters, when and why frauds are committed. Various theories have attempted to explain the causes of fraud and the two most cited theories are the Fraud Triangle Theory (FTT) of Cressey (1950) and Fraud Diamond Theory (FDT) of Wolfe and Hermanson (2004). Both of them identify the elements that lead perpetrators to commit fraud.

2.2.2 The Fraud Triangle Theory

Donald Cressey (1950), a criminologist, started the study of fraud by arguing that there must be a reason behind everything people do. Questions such as why people commit fraud led him to focus his research on what drives people to violate trust?

The three elements of fraud summarized by Cressey (1953) are commonly presented in a triangular diagram. The top element of the diagram represents the pressure or motive to commit the fraudulent act while the two elements at the bottom are perceived opportunity and rationalization.

Perceived Pressure

Perceived pressure refers to the factors that lead to unethical behaviours. Every fraud perpetrator faces some pressure to commit unethical behaviour (Abdullahi and Mansor, 2015a). These pressures can either be financial of non-financial pressures. Albrecht et al. (2006) pointed out that, since the pressure to commit fraud may not be real it is important to use the word perceived. If the perpetrators believed that they were pressurized, this belief could lead to fraud. Perceived pressure can exist in various ways, especially in non-sharable financial need. Financial pressure is recognized as the most common factor that lead an entity to engage in an evil action. Specifically, about 95% of all fraud cases have been perpetrated due to the fraudster's financial pressures (Albrecht et al., 2006). Vona (2008) further examines personal and corporate forces as motivations' proxies for fraud commitment. Examples of perceived pressure include greed, living beyond one's means, large expenses or personal debt, family financial problem or health, drug addiction and gambling.

Perceived Opportunity

The second necessary element of fraud to occur is perceived opportunity. Opportunity is created by ineffective control or governance system that allows an individual to commit organizational fraud. In the field of accounting, this is termed as internal control weaknesses. The concept of perceived opportunity suggests that people will take advantage of circumstances available to them (Kelly and Hartley, 2010). The nature of perceived opportunity is like perceived pressure in the sense that the opportunity does not have to be real too. However, the opportunity exists in the perception and belief of the perpetrator. In most cases, the lower the risk of being caught, the more likely it is that fraud will take place (Cressey 1953). Several factors lead to the existence of an opportunity to commit fraudulent activities in an organization such as negligence of employee's breach of policies and lack of disciplinary action. For example, if there is an inadequate job division, weak internal control, irregular audit, and the like, then the conditions will be favourable for the employee to commits fraud.

Rationalization

The rationalization is the third element of the fraud triangle theory. This concept indicates that the perpetrator must formulate some morally acceptable idea to him before engaging in unethical behaviour. Rationalization refers to the justification and excuses that the immoral conduct different from criminal activity. If an individual cannot justify dishonest actions, it is unlikely that he or she will engage in fraud. Some examples of rationalizations of fraudulent

behaviour include “I was only borrowing the money”, “I was entitled to the money because my employer is cheating me.” Additionally, some fraudster excuses their action as “I had to steal to provide for my family”, “some people did it why not me too” (Cressey, 1953). Rationalization is difficult to notice, as it is impossible to read the mind of the fraud perpetrator. Individuals who commit fraud possess a particular mind-set that allows them to justify or excuse their fraudulent actions (Hooper and Pornelli, 2010). Rationalization is a justification of fraudulent behaviour because of an employee’s lack of personal integrity, or moral reasoning

2.2.3 The Fraud Diamond Theory

In this theory, an element named capability has been added to the three initial fraud components of the fraud triangle theory above. Wolfe and Hermanson (2004) argued that although perceived pressure might coexist with an opportunity and a rationalization, it is unlikely for fraud to take place unless the fourth element (i.e., capability) is also present. In other words, the potential perpetrator must have the skills and ability to commit fraud.

Wolfe and Hermanson (2004) maintained that opportunity opens the doorway to fraud, and incentive (i.e. pressure) and rationalization lead a person toward the door. However, capability enables the person to recognize the open doorway as an opportunity and to take advantage of it by walking through repeatedly.

Capability

This is the situation of having the necessary traits or skills and abilities for the person to commit fraud. It is where the fraudster recognize the particular fraud opportunity and ability to turn it into reality. Position, intelligence, ego, coercion, deceit, and stress, are the supporting elements of capability (Wolfe and Hermanson 2004). Mackevicius and Giriunas (2013), not every person who possessed motivation, opportunities, and realization may commit fraud due to the lack of the capability to carry it out or to conceal it. Albrecht, Williams, and Wernz (1995) say that this element is of particular importance when it concerns a large-scale or long-term fraud. Furthermore, Albrecht et al. (1995) believe that only the person who has an extremely high capacity will be able to understand the existing internal control, to identify its weaknesses and to use them in planning the implementation of fraud. Similarly, Wilson (2004) discloses that rationalization and capability are all inter-related, and the strength of each element influences the others.

2.3 Empirical evidence

Under the empirical evidence are the studies that were made by some authors and were published. These include mainly case studies and surveys.

2.3.1 Articles on the role of computers in reducing fraud

Bhasin (2015b) remarked, "Technology is like a double-edged sword. On the one hand, perpetrators are using it to further fraudulent schemes; on the other hand, we are making some of our best progress using the same technology. Undoubtedly, technology can prove helpful in fraud detection and prevention in banks. As technology becomes more advanced, fraudulent schemes will become more complex, while more sophisticated fraud solutions will be developed to combat hackers' best efforts." But unfortunately, the fraud takes on many forms to be handled with any 'single' application or approach. The cat and mouse game will continue. As the landscape of fraud continues to shift, business leaders must be aware of trends and predictions that will allow them to implement internal/external controls and systems to help reduce the risk of fraud and keep them from becoming another statistic (Mueller, 2015). Instead of relying on reactive measures like whistleblowing, banks can and should take a more hands-on approach to fraud detection. A fraud detection and prevention program should include a range of approaches—from point-in-time to recurring and ultimately, continually for those areas where the risk of fraud warrants. Based on key risk indicators, point-in-time (or ad hock) testing will help identify transactions to be investigated. If that testing reveals indicators of fraud, recurring testing or continuous analysis should be considered. By leveraging the power of data analysis software, banks can detect fraud sooner and reduce the negative impact of significant losses owing to fraud.

Magnitude of frauds in banks: The Indian Banking Industry scenario

According to Ernst & Young Report (E&Y 2012), "Different types of frauds caused Rs. 6,600 crore loss to the Indian economy in 2011-12, and banks were the most common victims in swindling cases; insider enabled fraud accounted for 61% of fraud cases." However, Soni and Soni (2013) concluded that "cyber fraud in the banking industry has emerged as a big problem and a cause of worry for this sector." Similarly, another survey conducted by Deloitte (2012) shows that "banks have witnessed a rise in the number of fraud incidents in the last one year, and the trend is likely to continue in the near future." The Deloitte India Banking Fraud Survey Report Edition II (2015) added "number of frauds in banking sector have increased by more than 10% over the last two years. Banks witnessed rise in level of

sophistication with which frauds were executed." It is universally accepted that continued prevalence of frauds will have long-term bad consequences for banks, customers, investors, government and the economy in general.

With the advent of mobile and internet banking, the number of banking frauds in the country is on the rise as banks are losing money to the tune of approximately Rs. 2,500 crore every year. While the figure for 2010-11 was Rs. 3,500 crore, for the current financial year (till September) it is about Rs. 1,800 crore. Further, state-wise list of information on banking frauds shows Maharashtra (Mumbai) reporting the highest number of cases to the RBI. In the last financial year, banks in the Maharashtra reported 1,179 cases with Rs. 1,141 crore being lost to such frauds. Maharashtra is followed by Uttar Pradesh with 385 cases during the same period. The RBI requires banks to pursue fraud cases vigorously with the CBI or police authorities, and in court. The central bank has taken several steps to sensitize banks and curb frauds in the banking industry. The evolving fraud landscape around banking and the increase in fraud-related losses requires automated detection systems and robust fraud defense processes (E&Y, 2010)

2.3.2 Articles on the forms of bank fraud

Ogundeji (2005) as cited by Nwanze (2006) gave the following types of bank fraud, executive, foreign exchange, domestic operations, reconciliation, money market and treasury, risk assets, information technology, financial control, clearing, fund transfer, teller operations and customer services related frauds. Olojo (2006) also described fraud typology as consisting of syndicated fraud, corporate fraud, executive fraud, internal fraud, external fraud, internal/external fraud, computer fraud, electricity failure aided fraud, good boy and good girl syndrome aided fraud, rotten leadership aided fraud, slow judicial aided fraud and survival politics induced aided fraud.

Also, Owho (2005) emphasized the following types of fraud, theft and embezzlement, defalcation, forgeries, suppression, fraudulent substitution, payment against uncleared effects, unauthorized lending, lending to ghost borrowers, kite flying and cross Firing, unofficial borrowing, foreign exchange malpractices, impersonation, over invoicing, manipulation of voucher, fictitious contracts, fictitious accounts, over valuation/under valuation of properties, false declaration of cash shortages, fraudulent use of bank documents, falsification of status report, misuse of suspense account, duplication of cheque books, drafts, mail transfers,

interception of clearing cheques, interception and switching of telex messages, inflation of statistical data, laundering, computer frauds, false proceeds of collection, robberies, teeming and lading, fake payment, claim of supernatural influence, and double pledging.

Discussion on Major Frauds and Forgeries in Nigerian Banking Industry

There are several types of fraudulent practices in the Nigerian banking industry, the domineering and prominent types are the one discussed under this heading. These types of fraud dominate the banking industry in frequency and the amount of money and losses sustained by the industry. The fraudulent practices include:

-Presentation of forged cheques and dividend warrants.

- Granting of unauthorized Loans
- Posting of fictitious credits
- Suppression of cheques and defalcating
- Fraudulent transfers and withdrawals
- Loss of money to armed robbers and
- Outright theft of money

It is observed that the trend at which the fraudulent withdrawal is increasing calls for a serious check. The rate is alarming and can be precarious and inimical to the survival of the present recapitalisation if the trend progresses unchecked.

2.3.3 Articles on the effectiveness of computers in reducing fraud

Computer intrusion

On Thursday, September 21, 2000, a 16-year-old boy was jailed for hacking into both the Pentagon and NASA computer systems. Between the 14th and 25th of October 2000 Microsoft security tracked the illegal activity of a hacker on the Microsoft Corporate Network. These examples illustrate that even exceptionally well protected domains can have their computer security compromised. Computer intrusion fraud is big business and computer intrusion detection is a hugely intensive area of research. Hackers can find passwords, read and change files, alter source code, read e-mails and so on. Denning (1997) listed eight kinds of computer intrusion. If the hackers can be prevented from penetrating the computer system or can be detected early enough, then such crime can be virtually eliminated. However, as with all fraud when the prizes are high, the attacks are adaptive and once one kind of

intrusion has been recognized the hacker will try a different route. Because of its importance, a great deal of effort has been put into developing intrusion detection methods, and there are several commercial products available, including Cisco secure intrusion detection system (CSIDS, 1999) and nextgeneration intrusion detection expert system (NIDES; Anderson, Frivold and Valdes, 1995).

Data mining

Data mining technique is a computer-aided fraud detection that is primarily used by fraud investigators and forensic accountants. (Albrecht and Albrecht, 2002) concluded that this method is a user-friendly, low-cost technique to evaluate the entire database. Moreover, this technique can help to avoid from making inaccurate generalizations based on limited information. However, this method is only suitable for a small company because data mining software does not efficiently process large volumes of information and does not allow programmers to focus suspicion on a specific type of fraud.

Continuous auditing

According to (Albrecht and Albrecht, 2002), continuous auditing can be done once computer queries and scripts are written. In fact, tests can be programmed into live corporate systems in order to provide continuous monitoring of transactions rather than audit on historical data during normal audit process. A number of companies have successfully used continuous monitoring.

Password protection

By ensuring that managers are capable of accessing into the user computer's security and auditing features, the use of password can assist them in preventing and detecting employees' fraud. This can be done by requiring a password before gaining access to functions that diverge from the standard procedure. In addition, to be more effective, the user password ought to be changed regularly. According to (Bierstaker et al., 2006) although passwords are the oldest line of computer defences, they still represent as the most effective and efficient mean in controlling access. The advanced technology in certain developed countries has built up new forms of password protection. The password employs biological features of the users or known as biometrics such as thumbprint, voiceprint, retina pattern and digital signature (Bierstaker et al., 2006).

2.4Summary

Chapter 2, literature review, was gathered in a manner so that the researcher will have a better understanding and increase knowledge on the area of study. This chapter looks at literature review which is composed of conceptual framework, theoretical and empirical evidence. The next chapter is going to cover data presentation, analysis and discussion. The last chapter, Chapter 5, will cover the summary of the research, conclusion and recommendations.

CHAPTER III

RESEARCH METHODOLOGY

3.0 Introduction

This chapter will focus on research design, population of the study, sample size research instruments, and data sampling and analysis to be used in the research study.

3.1 Research Design and justification

The researcher used a descriptive research design in form of a case study. The descriptive research design allowed the researcher to carry out a study by questioning of individual units from a population and associated techniques of data collection such as questionnaire construction and methods for improving the number and accuracy of responses, data with techniques such as comparison, measurement, classification and evaluation.

3.2 Target Population

The target population in this study comprised of bank managers, bank tellers, and security from Ecobank Bindura

3.3 Sampling Techniques

A sampling technique is a method used to come up with the sample size being used by the researcher in coming up with a sample that have approximately the same characteristics as closely as possible (Crawshaw and Chambers, 2001). In this study the researcher used stratified random sampling and judgemental sampling.

3.4 Sample Size

Sample size refers to the number of participants or observations included in a research. This number is usually represented by n. Therefore the sample size for this research was six.

3.5 Research Instruments

Kothari (2004) instruments in research are tools or equipment that are used to collect data for example, questionnaires, interviews and observation. In this study the researcher used questionnaires and interviews to gather data.

3.5.1 Advantages and disadvantages of interviews

- Interviews provided social cues. Social cues, such as voice, intonation, body language etc. of the interviewee gave the interviewer a lot of extra information that added to the verbal answer of the interviewee on a question
- interviews had no significant time delay between question and answer; the interviewer and interviewee directly communicated with each other
- The answers of the interviewees were more spontaneous, without any extended reflections.
- However, interviews were time consuming and came up with a lot of costs. Interviewing an interviewee in a place some 200 kilometers away would take a whole day, including travelling and interviewing.

3.5.2 Advantages of questionnaire

- It enabled collection of data from people who were be difficult to contact or to meet in person.
- It allowed uniformity in the way in which the questions are asked and hence making it reliable.
- A questionnaire gave respondents freedom because most respondents were more comfortable with facing a questionnaire other than the researcher.

Disadvantages of questionnaire

- Some people did not answer the questionnaire some even answered half of it which there gave the researcher difficulties in analyzing the outcome
- The researcher was not sure that the right people complete the questionnaire
- Some people take did not take the questionnaire seriously

3.6 Validity and Reliability

As illustrated by Zikmund (2005) validity is the exactness of a measure or degree to which a source truthfully represents a concept. Validity ensures the ability of a scale to measure intended concepts. The utilisation of various information accumulation strategies within the study ensured that the gathered information was consistent and true. The researcher utilised

both subjective and quantitative research which ensured validity. Reliability means how predictable the discoveries depend on the techniques for information gathering and examination. Individual meetings were conducted alongside the questionnaire to measure reliability.

3.7 Data Collection Procedures

These are steps followed by the researcher to administer instruments and collect data respondents. The researcher personally distributed and collected questionnaires from the respondents. Reminders were periodically sent to the respondents for the date of collection of the questionnaire. The respondents of the interviews were informed of the interview before conducting them.

3.8 Data Presentation and Analysis

Data presentation is the manner in which data is to be displayed. Data was displayed using graphics, tables and charts in order to make the data more understandable. The researcher used pie charts, tables and bar graphs to present and analyse the data. Data analysis is a process of systematically applying logical and or statistical techniques to evaluate and describe data. All questionnaires were checked for physical completeness. Content analysis was used to analyse qualitative data from open ended questions. Deductive data analysis approach was used and the researcher interpreted data from general to particular. Microsoft excel package was be used as a major tool for tabular and graphical presentations.

3.9 Ethical Considerations

These are codes of conduct which are regarded as appropriate to academics during the research study. The researcher ensured that all participants were well informed about the nature of the study and its purpose. The researcher also assured the respondents that the research would strictly abide to all ethical guidelines such as confidentiality and honesty.

3.10 Summary

This chapter looked at research methodology, research design, target population, sample size, sampling techniques, research instruments, data collection procedures and data presentation, analyses and procedures. The purpose of this section is to set the standards high to ensure that gathered data is valuable and useful.

CHAPTER IV

DATA PRESENTATION, INTEPRETATION AND DISCUSSION

4.0 Introduction

The previous chapter covered the research design, target population, sample size and sampling techniques, data collection procedures, research instruments, data presentation and analysis procedures. This chapter covers data presentation, interpretation and discussion of findings.

4.1Data presentation process

After having conducted interviews and collecting questionnaires, the researcher went through all the questionnaires to check for completion and errors. Questionnaires received were coded, edited and checked for incompleteness to make meaningful sense. The findings were then presented using pictorial and graphical techniques.

4.2 Response rate

4.2.1 Questionnaire response rate

Table 4.1Questionnaire response rate

Questionnaires issued	**Questionnaires received**	**Response percentage**
6	6	100%

Source: primary data

Of the six questionnaires that were issued to the bank personnel all of them were returned and were thoroughly examined for completeness and errors hence the response rate was 100%.

4.2.2 Interview response rate

Table 4.2 Interview response rate

Meetings planned	**Meetings held**	**Response rate**
6	5	83.33%

Source: primary data

There researcher organised to have six meetings for interviews however only five were held giving a response rate of 83.33%.This is because on the date that the meetings were held the undergraduate attachee at the bank was absent due to issues that were not disclosed.

4.3 Demographic details of respondents

The questionnaire helped to gather the demographic details of the respondents as they answered the questioned. These details include gender, age, highest educational level and length of service in the banking industry. These details therefore help in validating the data that would have been gathered through the questionnaires. Therefore the demographic details of the respondents are presented in Table 4.3 below.

Table 4.3 demographic details of respondents

Variable		**Number of respondents (n=6)**	
		Frequency	**Percentage (%)**
Gender	Male	4	57.14
	Female	3	42.86
Age	20-25 Years	1	14.29
	26 - 30 Years	-	-
	31 - 35 Years	2	28.57
	36-40 Years	1	14.29
	41 Years and above	3	42.86
Highest level of education	Ordinary Level	-	-
	Diploma	-	-
	Undergraduate	1	14.29

	Degree	5	71.43
	Masters	1	14.29
Length of service	Less than 5 years	3	42.86
	5-10 years	3	42.86
	11 years and above	1	14.29

Source: Primary Data

Gender of respondents

All respondents were Zimbabweans and majority being males accounting to 57.14% and 42.86% females. This shows that many of the responses in this research came from the male gender.

Age distribution of respondents

From Table 4.3 above, the majority of the respondents were in the range of 41 years and above which accounted to 42.86% of the respondents, followed by the age groups of between 31 and 35 years which encompassed 28.57% of the population, lastly the age group of between 20 and 25 years had 14.29% and between 36 and 40 years also had 14.29%. From this information it is evident that age was evenly distributed in the organisation.

Educational level

The sample consisted of individuals with high levels of literacy with 71.43% of the respondents having at least a degree, 14.29% with a masters degree and the other one was an undergraduate attachee (14.29%).

Length of service

From the table it is evident that only one person which is 14.29% of the respondents had been in the banking industry for over 11 years and 42.86% had been in the banking industry for less than 5 years and for the range of five to ten years there was also 42.86% of the respondents.

4.4 Data presentation and analysis

4.4.1 The role of computers in reducing fraud

The respondents were asked to indicate the effectiveness of computers in reducing fraud. The response rate is shown below in table 4.4

Table 4.4 role of computers in reducing fraud

n=6

The effectiveness of computers in reducing fraud	**Strongly disagree**	**Disagree**	**Agree**	**Neutral**	**Strongly agree**
Strengthens internal control	0	0	0	0	100%
Reduce financial problems	0	0	42.86%	0	57.14%
Analysis of crime	0	0	28.57%	0	71.43
Helps in investigation	0	0	0	0	100%

Source: primary data

From the results in table 4.4 above it is shown that the majority of the respondents accounting to 100% of the respondents strongly affirmed that computers are effective in reducing fraud because they aid in strengthening internal controls and help in the investigation process. Others went on to say that computers are effective in reducing fraud because with them is attached a huge set of evidence relating to crimes that can be committed using the computer, for example with the aid of a computer one is able to retrieve deleted fraudulent emails hence giving leads to the fraudster. However computer applications or soft wares can be manipulated then the effectiveness of computers in reducing fraud will be abridged.

57.14% of the respondents also strongly agreed that the use of computers aid in reducing financial problems (liquidity) in the bank and 42.46% also agreed. This is because through the use of computers people will be afraid of committing fraud in the bank due to fear of being detected this is because computers have a special advantage in detecting fraud as compared to the traditional ways of detecting fraud. Akinyomi (2012) supports this notion by arguing that bank frauds endanger organizational growth of a bank as it leads to bank distress. He also said that fraud reduces the deposits that can be made by depositors and ultimately leads to the erosion of the capital base of a bank, therefore by the use of computers in detecting fraud these effects will be reduced.

Adding on 71.43% of the respondents strongly agreed that computers are effective in reducing fraud because they assist in analysing the crime and also 28.57% agreed with this fact again. The respondents highlighted that computers help in analysing how fraud was committed and also be able to know the type of fraud committed in a bank. However to some extent the use of computers in analysing a crime of fraud committed may be ineffective this is

because the use of computers requires expertise and the fraudster will be an expert in computer use and may make sure not to leave any evidence that will give the investigators leads to the fraudster. This therefore means that computers should no stand alone as a measure to reduce fraud in a bank.

4.4.2 Prevalence rate of fraud in the bank

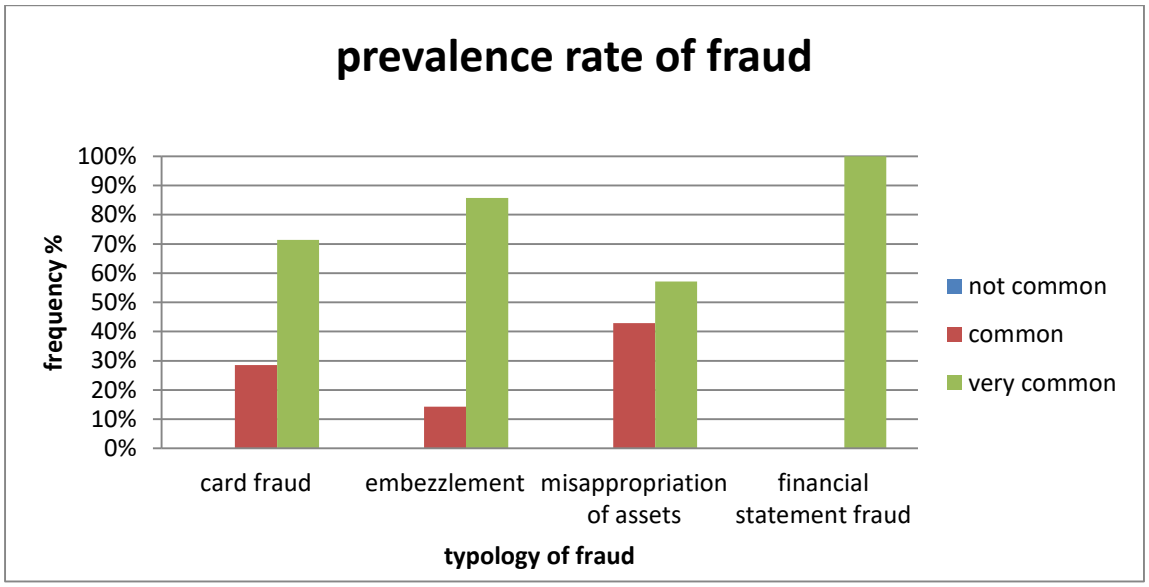

Fig 4.1 prevalence rate of fraud

The respondents were asked to highlight the prevalence rate of some typologies of fraud and the results came out as shown on the graph above.

100% of the respondents affirmed that financial statement fraud is very common in the banking sector. These findings seem to suggest that financial statement fraud incidences are being reported by banks, these findings are in agreement with the findings of the study carried out on Harare CBD banks by Njanike et al (2009) his study established 13 banks reported incidences of accounting fraud. Similar findings in these two studies are because of poor internal controls that are implemented. Employees are committing financial statement fraud because there is a lack or no segregation of duties and proper authorization. 71.43% of the respondents affirmed that card fraud is very common in the banking sector and 57.14% of the respondents agreed that misappropriation of assets is also very common in banks

85.71% also affirmed that embezzlement is very common in the banking sector. The respondents expressed their views on the prevalence of embezzlement in the Bindura banking sector and it obtained 85.71% indicating that respondents agreed that embezzlement is

prevalent in the banking sector. These findings relate to the findings of Idolor (2010) who asserts that embezzlement as a type of bank fraud is prevalent in many banking sectors. Furthermore Akinyomi (2012) in his study on Nigerian banks he identified that embezzlement was prevalent. Embezzlement is occurring in the banking sector because the employees are using company assets such as motor vehicles and think they are benefits of being a staff member.

4.5 Causes of fraud in the banking sector

Table 4.5 causes of fraud

Problem cause	**Strongly disagree**	**Disagree**	**Agree**	**Neutral**	**Strongly agree**
Poor internal control	0	0	0	0	100%
Financial problems	0	28.57%	42.86%	0	28.57%
Advance in technology	57.14%	14.29%	28.57%	0	0
Making up for being underpaid	0	42.86%	0	0	57.14%

Source: primary data

Table 4.5 above shows the summary of findings on various causes of bank frauds in commercial banks. Respondents expressed their views on poor internal controls as institutional causes of bank fraud and it obtained a 100% .This suggests that respondents strongly agreed that poor internal controls were causing bank fraud in the banking sector. This is supported by Akinyomi (2012) who asserts that poor internal controls and checks usually create a loophole for fraudulent staff, customers and non-customers to perpetrate fraud and in his study on Nigerian commercial banks, he established that poor internal controls were the major cause of fraud in banks.

28.57% disagreed that financial problems are a cause of fraud in the banking sector and 42.86% and the remaining 28.57% of the respondents agreed that financial problems are a cause of fraud in banks. This is usually because people would want to better their lives by gaining easy money. This can be related to the theory of rational choice theory which states that people are rational beings and they choose to pursue that which gives them greater utility.

While fraudsters are using sophisticated methods to gain access to credit card information, and perhaps penetrate fraud, new technologies are available to help banks prevent and detect fraud. Therefore 57.14% and 14.29% of the respondents disagreed that advances in technology are a cause of fraud, this is because the use of advanced technology enables securing of data through passwords and personal credential. However 28.57% agreed that advances in technology can be a cause of fraud, considering the age of the people responsible for facilitating electronic transactions, the management and the security personnel can devise ways of controlling possible cases of fraud. However from a sociological view it is assumed that the older generations have little knowledge on information and technology, thus making it possible for the relatively younger employees to deceive the older owners since they may not have the knowhow of the digitalised operations of the banking system.

More so, the majority of the respondents agreed that making up for being underpaid is another cause of fraudulent activities in a bank. The findings revealed that most of the respondents were aware that making up for being underpaid is playing a pivotal role in promoting fraudulent activities in banks. This was supported by Siegel (1992) who postulated that crime is an outcome of weighing two decisions and choosing the best in regards to the individual making the decision. He further states that when the possibility of reaching success financially eliminates the struggle of not having that success, people will commit fraud this shows that committing fraud is as a result of making a rational decision.

New ideas on the causes of fraudulent activities in banks were brought up during interviews which were conducted by the researcher. The respondents revealed that lack of good corporate governance is also causing people to commit fraud. This can be related to the Agency Theory by Jensen et al (1976) whereby they said top management abuses their position of trust for their personal gains, poor governance is a trait that has been accepted and made part of the nature of business in the banking industry.

Employee conspiracy (collusion) was said to be another cause of fraud and this is due to the fact that fraud is a complicated crime that in most cases can hardly be committed by single person with greatest assurance of success. However through collusion of employees fraud can be determined to occur successfully with little detection. This is in support of what was said by Sutherland (1949) in his differential association theory, that criminal behaviour is learned from interaction with others and it takes place when what has been learned inclines one more towards committing crime than not committing the crime.

4.6 Factors that enhance the effectiveness of computers in reducing fraud in the banking sector.

Respondents highlighted factors that enhance the effectiveness of computers in reducing fraud. These factors are presented in Table 4.6 below.

These included advance in technology where 71.43% of the respondents affirmed that advance in technology enhances the effectiveness of computers in reducing fraud in the banking sector as fraudsters may have knew techniques which therefore needs the technology to be tracking with the modus operandi of perpetrators. However 28.57% of the respondents said advance in technology hinders the effectiveness of computers in reducing fraud because high levels of expertise will be required for the mechanisms to be effective.

100% of the respondents affirmed that internet banking helps to enhance the effectiveness of computers in reducing. This is highly due to the fact that when using internet banking there is no need for a person to physically visit the bank and the credentials will be secured with passwords that are confidentially secured.

Also 100% of the respondents highlighted that employee motivation can also enhance the effectiveness of computers in reducing fraud. This is because when employees are motivated they do their job willingly without any thoughts of defrauding the business hence the need for employee motivation.

Job rotation and effective communication also accumulated 100% support respectively from the respondents as factors that enhance the effectiveness of computers in fraud detection and prevention in the banking sector. There must be clear channels of communication upward, downward or across organisational levels, on any issues concerning fraud. This ensures a close relationship between the bank and its employees. Millichamp and Taylor (2008) supported the view that communication acts a pivotal role in an organisation.

Table 4.6 Factors that hinder or enhance the effectiveness of computers in reducing fraud

Problem cause	**Positive Effect**	**Negative Effect**
Poor internal control	-	7(100%)
Financial problems	-	7(100%)

Weakened society values	-	7(100%)
Job rotation	7(100%)	-
Advance in technology	5(71.43%)	2(28.57%)
Making up for being underpaid	3(42.86%)	4(57.14)
Internet banking	7(100%)	-
Employee motivation	7(100%)	-
Effective communication	7(100%)	-

Source : primary data

4.7 Factors that hinder the effectiveness of computers in reducing fraud in the banking sector.

Respondents were asked to give their view on factors that may affect the effectiveness of computers in reducing fraud either positively or negatively. These factors are presented in Table 4.6 above.

Poor internal controls were said to be the main factor that hinders the effectiveness of computers in reducing bank fraud as 100% of the respondents affirmed to that. In an organisation, to ensure an effective internal control system, communication should also be effective. There must be clear channels of communication upward, downward or across organisational levels, on any issues concerning fraud. This ensures a close relationship between the bank and its employees. Millichamp and Taylor (2008) supported the view that communication acts a pivotal role in an organisation. Communication makes it easier for auditors to obtain full understanding of the business processes such as procedures used to record transactions, classes of transactions and processes used by the bank in preparing its financial statements. This therefore means that poor internal controls and poor communication affect the effectiveness of computers in reducing fraud.

The respondents also highlighted that financial problems and weakened societal values are also factors which negatively affect the effectiveness of computers in reducing fraud. They went on to say that as people are rational beings they can see much benefit in committing fraud than in not committing fraud either internally or externally. This can be drawn from Bentham (1789) who holds that a person is a rational actor when he or she seeks to maximise

his or her own utility in every situation. This means given two options a rational person will choose the option that most increases his or her own utility.100% of the respondents agreed that weakened societal values and financial problems hinder the effectiveness of computers in reducing fraud in the banking sector.in response to the interview questions the respondents went on to highlight other mechanisms that can be used to curb fraud in addition to the use of computers.

Digital analysis was also suggested by the respondents as a method to combat fraud. However it was said to be the least effective method due to certain reasons. These reasons being: unfamiliarity of this analysis technique, and according to (Albrecht and Albrecht, 2002), although the digital analysis is easy to apply, this technique does not enable auditors to match the symptom found with the specific types of fraud.

More so, based on the interview findings, the respondents perceived bank reconciliation as the most effective method to combat fraud due to lots of transactions involving huge amounts of cash. Thus, by preparing reconciliations on a regular basis, it will help to ensure that cash is not stolen and served as a mean of identifying and fixing accounting errors or un-posted bank transactions. In comparison, the findings by (Bierstaker et al., 2006) showed that bank reconciliation was rated at the ninth most effective technique perceived by the respondents.

In response to the open-ended question on what should be done by banks to curb fraud, several suggestions were made by the respondents. The suggestions include: educate and create awareness among the staff on integrity, foster ethical values, focus on fraud prevention, establish a proper written policy and procedure, maintain the adequacy and effectiveness of control, reduce politics and make use of whistleblowing.

4.8 Chapter summary

This chapter has discussed the results, interpreted them and outlined the major findings of the study. The findings were then compiled from the research instruments which were used in this research (questionnaires and interviews). The next chapter will focus on the summary of major findings, conclusions and recommendations of the study. Suggestions for further research will also be highlighted.

CHAPTER V

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction

The previous chapter presented the findings of this study. Therefore this chapter looked at the summary of the findings in relation to the research objectives, conclusions which summarize the whole project, the recommendations from the findings and suggestions for further research.

5.1 Summary of Findings

After analysing the results of the study in previous chapter, the following findings were noted:

The study aimed at evaluating the effectiveness of computers in managing bank fraud. Findings from the study revealed that computers enhance chances that an offender can be detected. It was established that due to the initiation of new technology in the banking systems, computers act as a measure in preventing and detecting fraud. The researcher was specifically focusing on banks in Bindura Central Business District. The researcher used questionnaires and interviews to collect data

The study established that computers assist in the detection and prevention of fraud in banks. Respondents further agreed that computers are very crucial as they can supply with clues or leads that may assist and direct the investigation process.

It was found out that financial statement fraud is the most prevalent type of fraud in the banking industry. And the other types of fraud that are prevalent in the banking sector are embezzlement, card fraud and misappropriation of assets respectively.

However, respondents expressed their views on the factors that hinder the effectiveness of computers as a way of detecting and preventing fraud in banks. This can be attributed to the fact that the extensive use of computers in banks can result in new complex methods of committing fraud to the extent that the knowhow is only available to the people who would have committed the fraud using computers hence the ineffectiveness of computers in detection and prevention of fraud.

The study further revealed several factors which enhance the effectiveness of computers in managing bank fraud. The factors which were considered by the respondents as enhancing were advancement in the technology that is being used by the banks to more secure systems and the use of internet banking which secures credentials of clients. The majority agreed that these can positively affect the effectiveness of computers in detecting and preventing fraud. As indicated by findings in the previous chapter that poor internal controls, financial problems and weakened societal values may hinder the effectiveness of computers in managing bank fraud as the people's behaviour will be driven by their need for money.

The majority of the respondents also argued that there are various ways to improve the effectiveness of computers in the prevention and detection of fraud, these include continuous maintenance of systems, educating clients about the advantages of internet banking, and strong internal controls.

5.2 Conclusion

This study gave enough evidence to show that computers are an effective way to prevent and detect fraud in the banking industry. This is because most respondents claimed that computers are a powerful tool in the detection of fraud due to the advances in technology in the economy .If computers detect fraud, they therefore prevent and also mitigate fraud in the banking sector. The researcher therefore concludes that the use of computers is an effective mechanism in detecting and preventing bank fraud. However the effectiveness of this mechanism is affected by several factors which hinder its effectiveness. Therefore for computers to be an effective mechanism in the detection and prevention of fraud there is need to make concentrated efforts in minimising factors that affect their effectiveness.

5.3 Recommendations

In light of the above conclusions, it is recommended that;

- There is need for banks to use the fraud whistleblowing mechanism and protect the whistle blowers' identity and assure the parties that the information given will be treated in a confidential manner.
- Encouraging work environment which propels employees to follow established policies and procedures and operate in the best interest of the organization. Thus institutions should adopt sound corporate governance.

- Bank personnel should report allegations or concerns about fraud through favourable systems like the hotline or through an immediate supervisor. The available facilities must include secured telephone and fax lines as well as secured e-mail addresses.
- Banks should enforce effective internal controls thus bank managers and loss control department should work hand in hand to detect and reduce fraud.
- Banks should perform pre-employment screening especially when recruiting key personnel who supply them with the right information.
- Perform expected and unexpected audits. This helps to unearth any vulnerability and appraise the effectualness of the existing controls.
- The management of the banks must formulate and support a fraud policy which shall be the green book on management of fraud in banks.
- Top management of the banks must adopt sound corporate governance characterized by effective operational practices comparable to international standards as an essential ingredient for prevention of fraud in the banking sector.

5.4 Recommendations for future research

This study's main focus was on the effectiveness of computers in detecting and preventing fraud in banks. It is recommended that future research should look at the following; other crimes apart from fraud that are committed in the banking industry. There is also the need to extensively look at fraud causation and management to establish some policies that banks and other business organizations can abide to in order to control fraud.

REFERENCES

Abdullahi, R. and Mansor, N. (2015a). Concomitant Debacle of Fraud Incidences in the Nigeria Public Sector: Understanding the Power of Fraud Triangle Theory. International Journal of Academic Research in Business and Social Sciences, Vol. 5, No. 5, pp, 312-326.

Abdullahi, R. and Mansor, N. (2015b). Forensic Accounting and Fraud Risk Factors: The Influence of Fraud Diamond Theory. The American Journal of Innovative Research and Applied Sciences. 1(5):186-192.

Association of Certified Fraud Examiners (ACFE). 2004. 2004 Report to the Nation on Occupational Fraud and Abuse. Austin, TX: ACFE.

Akinyomi, O. J., 2012. Examination of fraud in the Nigerian Banking Sector and its prevention: Asian Journal of Management research volume 3(1): 184-192

Albrecht, W.S, Albrecht, C. C and Albrecht, C. O., 2006. Fraud Examinantion, New York: Thomson South Western.

Albrecht, W.S, Albrecht, C. C and Albrecht, C. O., 2008. Current Trends in fraud and its detection: A global Perspective Information Security Journal Vol.17. Retrieved from www.ebscohost.com on 11/06/2014.

Beirne, Piers, James, Messerchmidt., 2000. Criminology. Westview Press. ISBN 0-15-501926.

Cooper, D and Schindler, P., 2008. Marketing Research Boston: McGraw Hill.

Cressey, D. R., 1953. Other People's Money. Montclair, NJ: Patterson Smith pp1-300.

Davies, J. H., Schoolarman, F. D., &Donaldson, L.1997. Toward a stewardship theory of management. Academy of Management Review, 22: 20-47.

Davies, H., 1996. Financial Regulation: Why, How and by Whom? Speech by the Deputy Governor Bank of England at the CIBEF Inaugural Lecture, John Moores University.

Dooley, D. 2004. Social Research Methods. Englewood Cliffs, Prentice Hall. Dentler, R. A., 1967. Major Social Problems Chicago: Rand Mc Nally and Company.

Dorminey, J., Fleming, A., Kranacher, M., and Riley, R., 2010. Beyond the fraud triangle: The CPA Journal, 80(87), 17-23. Federal Bureau of Investigations, U.S Department of Justice, 1989; 3. White Collar Crime: A report to the public Washington DC. Government Print.

Levi, M. (2008). Organized frauds and organizing frauds: unpacking the research on networks and organization. Journal of Criminology and Criminal Justice, (7), 389-419.

Lister, L. M. (2007). A Practical Approach to Fraud Risk: Internal Auditors.

Onuorah and Ebimobowei. 2012. 'Fraudulent activities and forensic accounting services of banks in Port Harcourt, Nigeria.': Asian Journal of Business Management, Vol.4, issue 2.

Rasha, K., & Andrew, H. (2012). The New Fraud Triangle, Journal of Emerging Trends in Economics and Management Sciences, Vol. 3(3): Retrieved from google.com July 13, 2014.

Rezaee, Z., Crumbley, D. L., & Elmore, R. C. (2004). Forensic accounting education. Advances in Accounting Education: Teaching and Curriculum Innovations, Vol. 6, pp. 193-231.

Singleton, T. W., Bologna, G. J., Lindquist, R. J., & Singleton, A. J. (2006). Fraud auditing and forensic accounting, 3rd Ed., John Wiley & Sons, Inc, New Jersey.

Smith, M., Omar, N., Sayed, I. S. I. and Baharuddin, I. (2005). Auditors' perception of fraud risk indicators: Malaysian Evidence. Managerial Auditing Journal , Vol. 20, No. 1, 73-85.

Srivastava, R. P., Mock T. J., & Turner, J. L. (2005). Fraud Risk Formulas for Financial Statement Audits. Australian National University Business and Information Management Auditing Research Workshop and from Gary Monroe, Lei Gao and Lili Sun. pp. 1-48

Thanasak, R. (2013). The Fraud Factors. International Journal of Management and Administrative Sciences (IJMAS) (ISSN: 2225-7225) Vol. 2, No. 2, pp. 01-05.

Vance, S. (1983). Corporate leadership: Boards, directors and strategy. New York: McGraw-Hill.

Vona, I. W. (2008). Fraud Risk Assessment: Building a Fraud Audit Programme: Hoboken, New Jersey: John Wiley and Sons.

Wells, J. T. (2005). Principles of fraud examination. Hoboken, N.J.: John Wiley & Sons Inc.

Wells, J. T. (2011). Corporate Fraud Handbook: Prevention and Detection: 3rd Edition: Hoboken, New Jersey: John Wiley & Sons Inc.

Wilks, T. J., & Zimbelman, M. F. (2004). Decomposition of Fraud-Risk Assessments and Auditors' Sensitivity to Fraud Cues. Contemporary Accounting Research, 21(3), 719-745.

Wilson, I. (2007), Regulatory and institutional challenges of corporate governance in Nigeria post consolidation. Nigerian Economic Summit Group (NESG) Economic Indicators, April-June, Vol. 12, No 2

Wolfe, D., & Hermanson, D. R. (2004). The fraud diamond: Considering four elements of fraud. The CPA Journal, 74 (12), 38-42.

APPENDIX A: QUESTIONNAIRE

I Thelma Salatiele am a student at Bindura University of Science Education carrying out a research in partial fulfilment of the requirements of Bachelor of Commerce Honours Degree in Financial Intelligence. I am investigating the effectiveness of computers in reducing fraud in banks. May you kindly respond to the following questions as honestly as possible. Your response will be mostly appreciated and will be treated with confidentiality.

Instructions to respondents

1. Please do not write your name.

2. Kindly answer all questions.

3. Please tick where applicable in the boxes provided and explain briefly further where blank spaces are provided if necessary.

SECTION A: DEMOGRAPHIC DETAILS

Tick where appropriate

1. What is your sex? male [ ] female [ ]

2. What is your age group?

20-25years [ ] 26-30years [ ]
31-35years [ ] 36-40years [ ]
41years and above [ ]

3. What is the length of your service in the Banking industry?

Less than 5 years [ ] 11years and above [ ]
5-10 years [ ]

4. What is your level of education?

Ordinary level [ ] Advanced level [ ]
Diploma level [ ] Degree level [ ]

If other please specify…….
…….

SECTION B : WHAT IS THE ROLE OF COMPUTERS IN REDUCING FRAUD IN YOUR BANK?

5. Below is a list of mechanisms which can be used to measure the effectiveness of computers in reducing bank fraud? For each item, please indicate how you agree that it contributes to reducing fraud in your bank.

The effectiveness of computers in reducing fraud	**Strongly disagree**	**Disagree**	**Agree**	**Neutral**	**Strongly agree**
Strengthens internal control					
Reduce financial problems					
Analysis of crime					
Helps in investigation					

If you have another opinion please specify……...

6. Indicate the prevalence rate of the following typologies of fraud in the banking sector?

Type of fraud	**NOT COMMON**	**COMMON**	**VERY COMMON**
Card fraud			
Embezzlement			
Misappropriation of assets			
Financial statement fraud			

If there are any other specific types please specify……

SECTION C: THE EFFECTIVENESS OF COMPUTERS IN REDUCTION OF FRAUD

7. Have there been any cases of fraud in your bank? **Please tick** yes [ ] no [ ]

8. Please indicate the prevalence rate of fraud in your bank **by ticking where appropriate**

Very low [ ] low [ ] moderate [ ] high [ ]
very high [ ] extremely high [ ]

9. To what extend do you agree with the following as the causes of fraud the banking sector?

Problem cause	**Strongly disagree**	**Disagree**	**Agree**	**Neutral**	**Strongly agree**
Poor internal control					
Financial problems					
Advance in technology					
Making up for being underpaid					

If not mentioned please specify……

10. Which factors hinder or enhance the effectiveness of computers in reducing fraud?

In this section you are asked to give your opinion on the factors that affect the effectiveness of computers in reducing fraud in the banking sector.

Tick where appropriate

Problem cause	**Positive effect**	**Negative Effect**
Poor internal control		
Financial problems		

Weakened society values		
Everybody else is doing it		
Advance in technology		
Making up for being underpaid		
Internet banking		

If there are any other factors please specify……

APPENDIX B: INTERVIEW GUIDE

1. What is the role of computers in fraud management?
2. What can you say concerning the levels of bank fraud in Zimbabwe?
3. How effective are computers in reducing bank fraud?
4. Briefly can you give factors hindering the effectiveness of computers in reducing fraud in Zimbabwean banks?
5. What are the factors which enhance the effectiveness of computers in reducing bank fraud?
6. In your opinion, what do you think should be done by banks to curb fraud?
7. What do you think should be done to improve the effectiveness of computers in reducing bank fraud in Zimbabwe?