BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF COMMERCE

DEPARTMENT OF INTELLIGENCE AND SECURITY STUDIES

MANAGING FRAUD USING INTERNAL CONTROLS: - A CASE STUDY OF SIMBISA BRANDS LTD FAST FOODS RETAIL SECTOR (PERIOD 2021-2022)

BY

PRINCE ITAI CHAMBOKO

(B193449B)

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.

JUNE 2023

Release Form

Name of Author:	Chamboko Prince I
Title of Project:	Managing fraud using internal controls: - A case study of Simbisa Brands Ltd fast foods retail sector (Period 2021-2022)
Degree Programme:	**Bachelor of Commerce (Honours) in Financial Intelligence**
Year submitted:	**2023**

Permission is hereby granted to Bindura University of Science Education to produce single copies of this research project for private scholarly research purposes only.

Signed: …………………………………… Date: ……………………………………….

Approval Form

The undersigned certify that they have read and recommend Bindura University of Science Education for acceptance, a research project entitled: "**MANAGING FRAUD USING INTERNAL CONTROLS: - A CASE STUDY OF SIMBISA BRANDS LTD FAST FOODS RETAIL SECTOR (PERIOD 2021-2022)**", submitted by Prince Itai Chamboko in partial fulfilment of the requirements of the Bachelor of Commerce (Honour's) Degree in Financial Intelligence.

I. To be completed by student.

I certify that this dissertation meets the preparation guidelines as presented in the Faculty Guide and Instructions for typing dissertations

Signature of student….…………………. Date ………………….

II. To be completed by supervisor.

This dissertation is suitable for submission to the faculty. This dissertation should be checked for conformity with Faculty guidelines.

Signature of Supervisor……………………. Date……………….

III. To be completed by Chair of Department.

I certify to the best of my knowledge that the required procedures have been followed and the preparation criteria has been met for this dissertation.

Signature of Chairman……………………. Date…………….

Declaration

I Chamboko Prince Itai (B193449B) declare this research project as my own work and have not copied or lifted from any source without the acknowledgement of the source.

Signed…………………………….

Date……………………………….

Dedication

To my parents, who have been my constant source of motivation and inspiration. Without their unwavering support and encouragement, I would have never been able to achieve my academic goals.

To my one and only little sister Princess, who has always been proud of my achievements and cheered me on relentlessly. Your unwavering faith in my abilities has been instrumental in my success.

And finally, to my mentors, who have challenged me to expand my horizons and pushed me to reach for the stars. Your guidance and expertise have led me to this point, and I am deeply grateful for your contributions to my education.

Thank you all for everything you have done to help me achieve this remarkable milestone. Without you all, this would not have been possible.

Abstract

The objective of this thesis will be to manage fraud using internal controls in the fast-foods restaurant (Simbisa Brands ltd). The aim of this research study was to investigate the effectiveness of internal control measures as a means of managing fraud within Simbisa Brands between 2021 and 2022. A descriptive study design was utilized for the research study with a sample size of 52 participants. The sample consisted of 11 participants who were interviewed, and 41 who completed a questionnaire survey that was designed based on the COSO framework. A thorough analysis of the responses was conducted using descriptive statistics within SPSS and the results were presented through tables, pie charts and graphs. It was found that Simbisa Brands had implemented internal control procedures to prevent fraud, but there were still some gaps in the system. The most significant challenges were noted to be skimming, financial statement fraud and electronic card fraud. It was also observed that there was a lack of awareness among employees in relation to the internal control procedures, leading to their failure to comply with the set rules and regulations. Based on the research findings, this study proposed a series of recommendations to manage fraud within Simbisa Brands. These included the need to enhance employee awareness of the internal control procedures through regular training sessions, establishment of independent internal audit function, and strengthening the collusion prevention mechanism through separation of duties. Overall, this study demonstrates the importance of implementing effective internal controls in managing fraud within organizations, and provides valuable insights into how Simbisa Brands (Quick Service Restaurants) can mitigate fraud risk.

Acknowledgements

I want to start by expressing my gratitude, honor, and sincere gratitude to the All-powerful, the great knowing and the omnipotence God for providing excellent health, stamina and not forgetting the flawless knowledge provided during my studies. There would have been no progress without him.

I would very much like to express my authentic gratitude and appreciation to my supervisor, Mr. F. Chituma, for his constant commitment, invaluable guidance, intellectual leadership, inspiring encouragement to never stop dreaming big in every aspect of life, and for providing feedback on each part of this research report.

Additionally, my sincere gratitude to Simbisa Brands' management can never be enough for letting me carry out this task within the confines of their company. Additionally, I want to express my gratitude to all of the staff members from the chosen departments for their valuable assistance.

Last but not least, I want to express my gratitude to my fellow students at Bindura University of Science Education for their assistance, support, and close collaboration during my studies.

Table of Contents

List of Tables

List of Figures

List of Appendices

CHAPTER ONE

1.0 INTRODUCTION

Regardless of the size, nature, or industry in which an organization operates, it is constantly vulnerable to fraud. Fraud has been the cause of the closure and failure of many businesses around the world, as evidenced by the occurrence of global cases such as the Enron, Tyco, and WorldCom scandals, (Fusaro, et al., 2002). While advances in technology and improved use of advanced technology have assisted criminals in escaping fraud, it has been demonstrated that the same technology can be used to help curb fraud. Companies, particularly those operating in emerging markets, may suffer revenue losses if strong detection and deterrence measures are not implemented. The implementation of internal controls, according to (Arwinge, et al., 2013), has attracted a lot of attention on a global scale. According to Pickett (2012), the modern workplace's transience and narrowing hierarchy have increased the risk of fraud, putting organizations at greater risk for fraud. As a result of these catastrophes, organizations have turned to modern technologies to combat fraud. Ribeiro, et al., 2021 these'd that using technologies such as artificial intelligence, data analysis, robotic process automation (RPA), and cyber forensics can be extremely beneficial in combating fraud. According to the Association of Certified Fraud Examiner/s (ACFE), firms lose up to 5% of their hard-earned income to fraud each year, totaling US$3.7 trillion globally.

1.1 Background to the study

Generally, the world of commerce has not been at ease, with the skyrocketing of commercial crime such as fraud, also regulatory pressure on financial institutions to curb fraud has substantially increased. Generally, fraud is any act that leverages falsehood to secure a gain. According to Black's Law Dictionary, fraud is defined as "a knowing distortion of the truth or concealment of a substantial fact to compel another to act to his or her detriment." Generically the prevalence of fraud in the retail store industry has received substantial attention as a result of general corporate scandals like Enron, World Co, and the most recent Steinhoff disaster, as well as a new influx of laws and legislation intended to strengthen the transparency of financial information. Fraud has led to the closing of many retail businesses even to the extent of bankruptcy. Generally, Zimbabwe has not lagged behind this trend as many shops, stores, and supermarkets in Harare Central Business District have in the past 5 years been affected by fraud and this has to stop as the adage goes on to say, "the first step to making money is to stop losing it".

The need to report on par sales results in the face of overwhelming competition, in accordance with research done in 2014 by Corporate Catalysts India Pvt Ltd, may lead businesses to use unethical business practices in order to survive in the market. Since fraud has a negative financial impact, undermines consumer confidence, and lowers branch value, it is a significant risk for the retail industry. Manufacturers, transporters, independent producers or subcontractors, packers, stock lists, wholesalers, and other third-party suppliers of services frequently used in the retail sector, which can significantly increase the possibility of collaborative fraudulent activity that is challenging to detect. According to the Deloitte India Fraud Study (2014), 54% of survey participants from the consumer product industry said that over the preceding two years, they have regularly dealt with fraud, merchandise diversion, bribery, and corruption.

The Institute of Internal Auditors (2019) reports that billions of dollars are squandered predominantly due to fraud and corruption, leading to inefficiency, project failure, financial difficulties, organizational complete collapse, and in the worst circumstances, humanitarian catastrophe. Internal controls that are poorly structured and ineffective governance that undermine the organization's procedures are frequently the source of fraudulent activities. The theory of fraud can be split into three categories: fraud against persons, external fraud, and internal fraud, also known as occupational fraud. Other variations of internal fraud include financial fraud, asset theft, and corruption. According to the Accounting of Europe 2019, the Grand Theft Auto project sees an annual loss of 50 billion euros through tax context, emphasizing the reality that fraud poses a threat to businesses. According to Pickett (2012), who downplays the severity of the fraud, even illicit funds from fraudulent enterprises have been used to support criminal crimes including human trafficking and drug trafficking. Asset misappropriation is the fraud kind that occurs the most frequently among the three categories mentioned above, thus according to ACFE, as of 2018.

1.2 Statement of the problem

The retail sector in Zimbabwe has long been hampered by fraud, left unchecked fraud can bring an organization to its knees (The Sunday Mail, 2023). The efficacy of control procedures in reducing fraud in fast food outlets is being questioned due to a recent increase in fraudulent activities in the retail sector. Organizations are becoming larger and more complicated, and as a result, people are frequently reduced to mere tools inside them. This has led to an increase in the specialized nature of work and the reliance on experts. A knowledge gap or restricted access to information, in turn, makes fraud detection more challenging. The probability of catastrophic fraudulent activity has increased due to recent information and technological revolutions. Fraud has not completely disappeared from the retail sector despite a clear emphasis on retailers adopting internal controls. The number of fraud incidents is increasing not only internationally but also in Zimbabwe.

On July 14, 2022, the internal auditor of Simbisa Brands received a complaint that an employee had been receiving cash payments in US dollars from customers between July 1 and July 14, and then converting the payments to local currency. The employee had allegedly been doing this to conceal the amount of cash received. During an audit, the internal auditor compared the bank statement against the till, which led to the discovery of the fraudulent activity

On another case three individuals who were employed as delivery personnel by Simbisa Brands and were given Total fuel cards to use for refueling their motorbikes. However, they allegedly withdrew cash from various Total service stations using the fuel cards and shared the money instead of using it for fuel as required by their employer. They reported to Simbisa Brands that they had used over $30,000 on the delivery bikes, but this was later found to be false after a tip-off was made to management. The police investigated the matter and recovered CCTV footage from various Total service stations, showing the three withdrawing cash instead of fuel. One of the individuals, Jackson, allegedly used some of the stolen money to buy a bike, which was also recovered by the police.

According to estimates, Zimbabwe Republic Police received (10 052) fraud cases in 2014 and (11 207) in 2015, representing an increase of 5.44% in fraud incidents. (ZIMSTATS 2019 Quarterly Digest). The aforementioned statistics show that fraud has been on the rise despite controls being in place in the retail sector. Analyzing the effectiveness of internal controls is, the contemporary issue that this study set out to answer.

1.3 Purpose of the Study

The subsequent research objectives will serve as a guide for the research.

1. To ascertain the nature of retail fraud in by Simbisa Brands for the period 2021-2022).
2. To identify the internal controls that are available in Simbisa Brands fast food outlets
3. To assess the incisiveness of the internal controls in Simbisa Brands
4. To propose areas where internal controls could be improved to reduce internal fraud.

1.4 Research Questions

1. Which type of fraudulent activities occurs in the Fast-food retail sector (Simbisa Brands)?
2. What are the readily implemented internal controls in Simbisa Brands?
3. How incisive are the internal controls available for curbing fraud?
4. What can be done by those in the fast-food retail sector for the refinement of internal controls?

1.5 The significance of the study

Due to the comprehensiveness of this study, the retail sector will benefit from it, through the demonstration of the value of internal controls in the industry. In addition, the research will uncover areas where the industry could be improved to reap the rewards of implementing internal controls. The government will also benefit from the areas that the study will identify as requiring policy scrutiny and an evaluation of the regulatory structure governing internal controls. Students studying at BUSE who might later want to conduct research in the same field will use the study as a source for their literature reviews. The study will be crucial in increasing public understanding of internal controls and how they can be utilized in Zimbabwe.

1.6 Assumptions

This research will be carried out on the assumptions that:

1. The respondents know about fraud; information from them will be accurate, complete, and relevant and therefore can be relied upon.
2. Fraud is occurring in the fast-food retail sector (Simbisa Brands).
3. The respondents will respond positively to the interviewer's questions.

1.7 Delimitations to the study

The primary goal of the study will be to manage fraud using internal controls. This study's main focus will be on the steps taken to curb and analyze how effectively they are reducing fraud in the retail sector. The research will answer questions on how incisive are the parameters set already, contributing to the reduction of fraud in the retail sector. It will go on to review the comments provided regarding the enhancements or adjustments of internal controls. Primary data and secondary data are the two types of data that will be used. Secondary data will be gathered through the use of offline, internet, journals, and textbooks, while primary data will be gathered through questionnaires and in-person interviews that will be conducted.

1.8 Limitations of the study

The researcher will have to rely on information that participants are willing to share and use primary and secondary data because some information will be deemed to be private and confidential and will not be made available to me. It is preferable to get certain facts or information from subject-matter experts. It will be difficult to get data from them because they will frequently be inaccessible; therefore, the researcher will make plans three days in advance to ensure the availability and stick to the time that will be stated to be free. The issue of confidentiality will be resolved by promising that the data they will provide will be kept private and used only for academic purposes.

1.9 Definition of terms

Fraud

According to Adeduro et al. (1998), intentional false representation, concealment, or omission of the truth to mislead or manipulate another person or a group of people financially, this might encompass activities such as misappropriation of assets and theft.

Ramamoorti (2008, p. 522) suggested that fraud comprises deliberate activities and is committed by people utilizing deceit, guile, and cunning, which may be broadly categorized as including two forms of misrepresentation: suggestio falsi (suggestion of untruth) or suppressio veri (suppression of truth).

According to Prabowo (2013), fraud has been present throughout history and is not a new phenomenon. Financial scandals have plagued the global economy since before the Industrial Revolution, as evidenced by cases dating back to the 1970s. For instance, the Equity Funding Scandal of the 1970s was one of the early major financial scams that involved the use of computers to aid in fraud perpetration (Pearson and Singleton, 2008).

Managing

Managing is the process of planning organizing, leading, and controlling organizational resources, it involves the art of employees and management colluding together to accomplish certain set goals and objectives through making use of the available resources efficiently and effectively. Managing encompasses a broad spectrum of the co-ordination of people, resources and processes to achieve set objectives.

Control Procedures

The Association of Fraud Examiners Report (1999) defines fraud prevention as a set of synchronized methods and tactics designed to impede, uncover, reduce, scrutinize, examine, police, and litigate incidences of fraud.

Case Study

A case study is an in-depth analysis of a particular situation or event, such a person, group, organization. It involves a detailed assessment of the subject of the study, using a variety of methods such as interviews, surveys, and observations (Creswell, 2018)

Internal Controls

The COSO Framework (2004), defines internal control as a procedure that is carried out by an entity's board of directors, management, and other staff members and with an intend to give sufficient guarantee pertaining to the accomplishment of business targets in efficacy and effectiveness of its functionality, dependability of financial statements, to ensuring that actions and behaviors are in accordance with relevant laws and regulations.

Internal controls have a vague definition. Internal controls vary among organizations and are used for various objectives. Measures and procedures that regulate a business's operations are generally referred to as internal controls (Ahok,2012).

Stamler et al. (2015) claim that these are preventative measures meant to thwart and hinder transactions through procedural demands for regular occurrences.

Michino (2011), explained that internal controls are those procedures that managers use to ensure that errors are prevented. Internal control is also defined as the systematic programs and procedures put in place by an organization's management to help it achieve its goals and objectives and comply with legal requirements (Njanike and Mutengezanwa, 2011).

1.10 Summary

The findings of this dissertation will demonstrate whether the measures taken to curb fraud by Quick Service Restaurants (Simbisa Brands) are effective enough. Chapter one has given a bird's eye view of the research and has established the foundation of succeeding chapters. The following chapter two will present the literature review from different authors. Chapter 3 to follow will discuss pertinent issues in the collection of data from the study's target population and its analyses. Presentation and analysis of data will be done in chapter four. Finally, chapter five will summarize, conclude, and make recommendations regarding the studied topic.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The intricacy of the retail industry in Zimbabwe leads to the emergence of several forms of economic crime. Due to this intricacy, several economic crimes have emerged (fraud). Owing to organizations' lack of pressure readiness, fraud has discovered a mechanism to unpredictably decapitalize firms.

2.2 Conceptual Framework

2.2.1 Defining Fraud

No rule that is generally applicable restricts fraud to a single general standard, claims Accountancy Europe (2017). Instead, there are many methods to describe fraud. Consolatory is the fact that financial crime is a catch-all term for various crimes including fraud and corruption and is defined and categorized by ACFE (2018) as a subclass of fraud.

According to the Association of Fraud Examiners (ACFE), fraud is any conduct that intentionally misrepresents the facts in order to benefit oneself. This definition was stressed in a 2004 report to the Nation on Occupational Fraud and Abuse. Fraud is defined as a deliberate invasion of truth to deceive another person in Webster's Ninth New Collegiate Dictionary (1990).

Fraud is defined as the knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment or a misrepresentation made recklessly without belief in its truth to induce another to act by Biegelman and Bartow (2012) on page 24 of Black's Law

Dictionary. Fraud is a general phrase that encompasses all types of deceptive tactics used by one person to gain an advantage over another, according to Webster's Ninth New Collegiate Dictionary. Therefore, there isn't a universally accepted definition of fraud that can be established because it encompasses all sneaky, devious, and unjust ways to defraud someone; the only limits that can be established by humans are those.

According to Albrecht (2003, 6), fraud is a type of deception that involves the following elements: a false representation made concerning a tangible aspect that is believed by the victim and used against them by the perpetrator. According to the ACFE, fraud also refers to the intentional misappropriation of resources or assets belonging to the employing entity in order to leverage one's position for personal benefit or profit.

According to Wells (2005, 8), fraud is any crime that involves dishonesty for financial benefit. According to common law, there must be four essential components for fraud to be established: a substantially deceptive assertion, knowing at the time of making it that the statement was untrue, reliance of the victim on the assertion, as well as losses brought on by the victim's reliance.

Zimmerman et al (2014) stated that the greatest fraud is the misuse of assets both cash and non-cash assets. Fraud is typically a social activity that can have significant economic repercussions for both businesses and individuals. Often triggered by a combination of greed and opportunity, it is like an infectious disease that can rapidly spread when circumstances allow for deception. The World Bank (2014) also defines fraud by implying that it is a form of action that involves the omitting or including a misrepresentation, a pretense of deceiving someone as a means to obtain a monetary or other benefit or to circumvent an obligation, or intentionally or recklessly misleading them.

The Securities and Exchange Commission (SEC) defines fraud as a type of illegal activity that involves transactions with securities. According to Section 10b-5 of the Security Exchange Act of 1934, it is illegal for anyone to utilize fraudulent tactics, false statements, or other artificial means to deceive others regarding material facts related to securities. Such activity is illegal whether it is carried out directly or indirectly, through the use of any medium of interstate commerce, mail, or exchange facilities of any national securities exchange.

In conclusion, fraud is the deliberate misrepresentation of a material fact that harms the victim. Generically fraud is accompanied by acts of deception, cunning, obscurity or an infringement of trust consciously either unintentionally to obtain a disproportionate or deceptive advantage (Stamler et al. 2015). Fraud requires several conditions to be met. They include having the purpose to deceive, making a materially false statement, knowing that the statement is false, having the victim rely on the erroneous(false) claim and ultimately experiencing adverse effects. (Wells 2012).

2.2.2 Internal and External Fraud

Internal fraud, external fraud, and fraud against people are the three categories into which fraud may be categorized, according to ACFE (2018). Data, assets, expenditures, and income are listed as the four primary goals of fraudsters by Pickett (2012). Furthermore, according to ACFE (2018), employees, managers, and company executives are all potential perpetrators of internal fraud. Internal fraud, also known as occupational fraud, is defined by ACFE as "the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets." The three subcategories of internal fraud identified by ACFE (2018) are asset theft, corruption, and financial statement fraud. On the other hand, external fraud may be committed by buyers, sellers, or other parties.

The ACFE defines external fraud as, among other things, dishonest consumers using forged payment information or dishonest vendors billing for items that haven't been delivered. Other parties may also commit crimes, such tax or loan fraud. The most typical form of internal fraud is asset theft (ACFE,2018). Asset misappropriation fraud involves outside parties or employees who take advantage of their status to commit fraud against the organization. Insider fraud is another name for it (Action Fraud, 2023).

Cash and non-cash asset schemes can be used to further categorize asset misappropriation scams. For instance, the ACFE claims that altering expenditure records and stealing corporate money are examples of asset misappropriation in businesses.

The Financial Stability Board (2014) elucidates that external fraud refers to the possibility of facing unanticipated financial, material, or reputation-based loss resulting from fraudulent actions carried out by individuals outside the organization. This risk category is widely acknowledged in regulatory frameworks worldwide, including Basel II/III standards.

2.2.3 Nature of fraud in the fast-food retail sector

On daily basis in each operation in the retail sector, acts of fraud are committed and these may look like they are insignificant to cripple a whole organization but when pragmatically calculated they prove to be decisive to an organization. In 2016 Boehmer argued that the retail sector is a multifaceted sector with a lot of activities going on, which makes it susceptible to fraudulent activities. Fraud is a pervasive issue that affects businesses in various industries, including the fast-food industry. Fraud can lead to significant financial losses, damage to a company's reputation, and legal consequences. In the fast-food industry, some common types of fraud include embezzlement, false refunds, inventory theft, procurement fraud, credit card fraud, vendor fraud, payroll fraud, and gift card fraud (KPMG, 2019). These types of fraud can occur at various stages of the business process, such as point of sale, inventory management, and payroll processing.

2.2.4 Procurement Fraud

Coenen (2011) these'd that procurement fraud is subject to corruption and bribery schemes. Generically procurement involves the bidding of goods and services through the process of acquiring a contract to supply goods or services to an organization. Coenen (2011) mentioned that the manipulation of the procurement process will be to generally gain an advantage in the bidding and the anomalous acts will ultimately result in an improper utilization of insider information and the use of duplicitous techniques to sway the process. According to Stamler et al. (2015), procurement fraud is the act of deceiving and manipulating invoices to obtain goods or services from a supplier with the knowledge of the supplier. This clearly indicates that the supplier and the company's agent will be networking together. Procurement fraud consists of a high depth of employee involvement and due to this it becomes difficult to detect its occurrence, the companies will not be willing to admit that their staff members are shirking their responsibilities as fiduciaries in order to further their own interests (Stamler, 2015).

Coenen 2011 also agrees with the view that procurement fraud is difficult to detect since management will have solicited with employees the personal benefits arising from procurement fraud being enhanced by insider relationships. The European Anti-Fraud Office (2020) posits that procurement fraud refers to the unlawful manipulation of a procurement process to secure contracts, goods, or services, or to gain an unjust advantage during the procurement process. There are several examples of procurement fraud schemes, including those that occur following the award of a contract, those that impact the bidding process, or both.

Collaboration among staff members and suppliers, supplier fraud against the business itself, and collusion among various suppliers or vendors are the three categories into which procurement can be divided. Supplier fraud against a company refers to when a supplier or vendor defrauds a retail store by using subpar replacements for goods, charging excessive prices, or participating in false billing schemes. Collusion between employees and vendors is done through the use of kickbacks, enticement, and bid manipulation.

2.2.5 Mobile Transaction Fraud

Au and Koffman (2008) defined mobile payment a form of digital payment transaction procedure in which at least the payer is involved who initiates a payment through the use of a mobile device in conjunction with a mobile network/communication to realize and authorize the transaction to the receiver. Au and Koffman (2008) discuss the emerging threat of mobile payment fraud. With the increasing popularity of mobile payments, the risk of fraudulent activities has also increased. Fraudsters are exploiting the vulnerability of mobile payment systems to carry out various fraud schemes, including skimming, phishing, and malware attacks. These attacks target user information, payment credentials, and funds, with the ultimate objective of illegal financial gain.

According to Au and Koffman (2008), the unique features of mobile payments, such as the use of wireless networks and the reliance on mobile devices' security, make them more susceptible to fraud than traditional payment systems. They suggest that the rapid development of mobile payment technology needs to be matched with robust security measures that consider both technical and non-technical factors. Au and Koffman (2008) argue that to prevent and manage mobile payment fraud, the industry must adopt a multi-layered approach that combines comprehensive security policies, customer education, and robust fraud detection and prevention technology. The authors emphasize the need for collaboration between stakeholders, including financial institutions, payment service providers, mobile network operators and regulators, to establish a unified approach to tackle mobile payment fraud. They conclude that sufficient measures must be implemented to ensure that mobile payments remain safe and secure for users.

As per the National Risk Assessment (NRA) Report of 2020, the employment of digital financial channels has led to the escalation of cyber risks, resulting in an approximate amount of US $900 million of unlawfully obtained gains annually in Zimbabwe. Additionally, the scarcity of physical currency in Zimbabwe has given rise to a surge in fraudulent activities associated with mobile payment systems, as indicated by a News24 report in 2018.

2.2.6 Electronic Card Fraud

Sudjianto (2010) argued that electronic payment fraud is any attempt by a criminal in trying to get a monetary benefit at the cost of the rightful owner of the card may it be a debit or credit card.

Sudjianto theses that card fraud can be subdivided into two that is theft of the actual card, secondly compromising the data associated with the account which includes the account number. In 2020 the RBZ instructed banks to review their preparedness for cyber security threats due to a 23% increase in electronic card frauds (Mudzingwa, 2020). Such statistical records on card fraud can cause the populace to have doubts about the use of electronic cards due to insecurity reasons.

Wendels (2009) stated that electronic card fraud can be a situation where the fraudster claims or assumes an erroneous persona or unauthorized access to another person's account. Generically identity theft is the possessing of one's information with the actual aim of defrauding the imitated personnel and then perpetrate an unlawful activity.

2.2.7 Asset Misappropriation and/or Embezzlement

According to J.H. Yamamura (2012), fraud that involves misappropriation of company assets can include asset theft and misuse. The Association of Certified Fraud Examiners (ACFE) reported that small businesses are the most common victims of asset misappropriation, with a median loss of $120,000. A lack of internal controls or bypassing them were cited as the main causes in 55% of cases. This type of fraud can lead to significant losses, reduced profitability, and even the closure of small businesses. Common examples of asset misappropriation include theft of cash or property, submitting fraudulent invoices or expense claims, check tampering, and payroll schemes. The ACFE reported that 45% of all economic fraud and crime resulted from asset misappropriation. Embezzlement, as defined by the FBI, involves deliberate misuse of money, property, or valuable items that have been entrusted to someone else's care for personal gain. Embezzlers often use a position of trust to take advantage of individuals who have entrusted them with property. Skimming and cash larceny are types of embezzlement that can occur in a business setting.

Skimming

Wells (2012) defines skimming as the theft of cash or accounts receivable by an employee after the sale has been recorded in the accounting system, which makes it difficult for the business owner to detect the fraud. He notes that the frequency of skimming has increased significantly due to the widespread use of electronic payment methods such as credit and debit cards. Skimming is particularly prevalent in industries such as retail, food service, and hospitality, where there is a high volume of cash and credit card transactions.

According to Wells (2012), skimming can take two forms: cash larceny and sales skimming. Cash larceny involves the theft of cash after it has been recorded in the accounting system, such as through the theft of deposits or cash register disbursements. Sales skimming, on the other hand, occurs when an employee steals cash or makes sales but does not record the transactions in the accounting system.

To prevent skimming, Wells (2012) recommends that business owners and managers implement strong internal controls, such as regularly reviewing account statements and monitoring cash registers and other point-of-sale equipment. They should also conduct background checks on all employees and provide employee training on fraud and theft prevention.

Coenen (2011) describes skimming as an embezzlement technique in which an employee steals cash before it is recorded in the accounting system. This is typically done by removing cash from receipts or other payment records before the documents are entered into the accounting system. As a result, the business owner may be unaware of the missing funds until much later.

According to Coenen (2011), skimming is a very difficult type of embezzlement to detect, especially in cases where the embezzler is in a position of trust such as a cashier, bank teller, or accountant. Skimming can also be difficult to detect because perpetrators may take small amounts of cash over a long period of time, making it less noticeable.

To prevent skimming, Coenen (2011) recommends strong internal controls such as segregation of duties and the use of electronic payment systems that leave an audit trail. She also suggests that businesses should regularly review financial statements and bank records to detect any discrepancies that could indicate skimming or other types of fraud. Overall, Coenen (2011) emphasizes the need for businesses to be vigilant and proactive in preventing and detecting skimming fraud.

Cash Larceny

Larceny fraud, also known as theft by false pretenses, is a type of theft in which the perpetrator fraudulently induces the victim to relinquish ownership of their property. In other words, the thief obtains the victim's property by tricking them into giving it up. (Cornell Law School, 2021).

Generically cash larceny involves the perpetrator taking cash generally that is not his or hers after the sale has been recorded by the victim (organization). Wells (2012) defined cash larceny as a situation by which subordinate purposefully withdraws cash from the employer without his/her consent or an agreement being reached between the two for such an act to be done. Larceny involves the perpetrator stealing the cash when the trail of its input has been recorded by the organization and this makes it difficult for the perpetrator to conceal the fraudulent activity done (Merriam-Webster, 2021).

2.2.8 Financial Statement Fraud

According to Wells, J.T. (2011), financial statement fraud involves the deliberate misstatement or omission of material information in a company's financial reports. This can include manipulating financial statements to show increased revenue or profits, hiding liabilities, or misrepresenting expenses to inflate earnings. Financial statement fraud is usually committed by senior management or executives, who have access to financial information and the power to make decisions that affect the company's financial reporting. This can be achieved through various methods such as understating expenses, overstating revenues, manipulating reserves, or misrepresenting assets or liabilities. Financial statement fraud has been a growing concern in recent years, with high-profile cases involving Enron, WorldCom, and Tyco International demonstrating the severe consequences of such fraudulent activities. Apart from criminal and regulatory penalties, financial statement fraud can also lead to a significant decline in stakeholder confidence, shareholder lawsuits, and even bankruptcy. According to a study by the Association of Certified Fraud Examiners, financial statement fraud cases have resulted in a median loss of $954,000, and the schemes last an average of 18 months before detection. Therefore, financial statement fraud is a serious issue that requires the attention of auditors, regulators, and executives.

2.2.9 The COSO Framework

The framework was first developed in 1992, and its most recent upgrade was made in May 2013. The fundamental ideas of the framework are lucidly described in updates. The 2013 framework may be used by organizations to create and execute internal controls in line with changing business and operating conditions. The new framework also makes it clearer how to assess if an internal control is successful and broadens the use of internal controls to satisfy operational and reporting goals. (Pathlock Team, 2021)

2.2.10 Internal Controls

COSO framework (2013), defines the internal controls as a process that is affected by the board of directors, management and other personnel that might include the audit committee (internal auditors) who need to provide reasonable assurance in regard to the objectives related to the operations, reporting and compliance. Internal control can be defined in a variety of ways. Various internal control functions can be used by various firms for various objectives. Generally speaking, internal control refers to procedures and policies used to keep an organization's activities under control (Ahokas, 2012). The idea of internal control was first established more than 100 years ago, but the relevance of internal control processes has grown over the last several decades, according to Arwinge et al. (2013).

According to Brown (1962), internal control was first acknowledged in 1905. This resulted from Lawrence Dicksee's 1905 work "Auditing," which discussed the responsibilities and procedures of an audit. Internal control was once frequently characterized as accounting controls, according to Maijoor (2000). He points out that the definition has since been expanded, and one that is more comprehensive is currently in use. Internal control's initial focus in the context of fraud, according to Dimitrijevic et al. (2015), was on fraud detection. They point out that as the breadth of internal control has expanded, so too has the emphasis switched from fraud detection to fraud prevention.

According to Coenen (2011), internal controls are essential in preventing and detecting fraud, including skimming. These controls are policies and procedures established by a business to ensure that assets are safeguarded, financial information is accurate and reliable, and operations are efficient and effective. Coenen (2011) identifies several internal control best practices that can help prevent and detect skimming. For instance, she recommends implementing segregation of duties, which involves separating job responsibilities between different employees to prevent any one person from having too much control over cash-handling or accounting functions. Other best practices she identifies include monitoring cash receipts and disbursements, using electronic payment methods, regularly reviewing financial statements and bank records, conducting background checks on employees, and creating a culture of honesty and ethics in the workplace.

According to Coenen (2011), implementing strong internal controls can help prevent and detect skimming and other types of fraud, but it requires a commitment from management and employees at all levels. She emphasizes the need for businesses to regularly review and update their internal control processes and for employees to be trained on how to identify and report suspicious activity.

2.3 Components of Internal Controls

The internal controls of an organization should encompass the following.

Control Environment

The control environment is a component of internal control that includes the organization's culture, ethics, and leadership. It sets the tone for the organization regarding how it conducts business and how it expects its employees and other stakeholders to act. An effective control environment promotes ethical behavior, accountability, and a commitment to doing what is right. An organization's control environment is affected by various factors, including the company's mission statement, leadership style, code of conduct, and employee training (KPMG, 2017).

Risk Assessment

Risk assessment is another crucial component of internal control. The risk assessment process involves identifying, analyzing, and evaluating the risks that the organization faces. The ultimate goal of risk assessment is to ensure that the organization can respond appropriately to potential risks while minimizing the possibility of negative consequences. Risk assessment involves identifying risks, evaluating the likelihood and potential impact of the risks, and prioritizing the risks based on their significance (Deloitte, 2015).

Control Activities

Control activities are the policies and procedures that the organization performs to achieve specific goals and objectives. These activities can be automated or performed manually, depending on the organization's operations. Control activities include a wide range of activities such as authorization, segregation of duties, reconciliation, and monitoring of transactions (COSO, 2013).

Information and Communication

Information and communication are a process of providing relevant, reliable, and timely financial and non-financial information to the relevant stakeholders within the organization. It involves the use of technology, reports, and other communication tools to ensure clear, concise, and accurate information that is easily understood by all stakeholders. Effective communication is essential in ensuring that every stakeholder understands their responsibilities and the organization's objectives (KPMG, 2017).

Monitoring Activities

Monitoring activities are the continuous assessment of the effectiveness and efficiency of internal controls. Monitoring activities include performing audits, analyzing data, and reviewing reports to identify potential control weaknesses. Continuous monitoring of internal controls is essential in ensuring that any weaknesses or issues are identified and addressed promptly (Deloitte, 2015).

2.4 Types of Internal Controls

Internal controls that are effective in the fast-food industry include segregation of duties, regular audits, strict inventory management, background checks, access controls, employee training, and surveillance and monitoring systems (KPMG, 2019). Segregation of duties involves assigning different tasks to different employees to reduce the risk of fraud. Regular audits involve conducting internal audits to identify any fraudulent activity and assess the effectiveness of internal controls. Strict inventory management involves maintaining accurate inventory records and conducting regular inventory checks to prevent inventory theft. Background checks involve screening job candidates before hiring to identify any criminal convictions or other red flags that could indicate a propensity for fraud. Access controls involve restricting access to sensitive areas such as cash registers, inventory storage, and computer systems. Employee training involves educating employees on fraud prevention and detection methods and providing a clear code of conduct that outlines the consequences of fraud. Surveillance and monitoring systems can help detect and prevent fraudulent activities by providing visual evidence of any suspicious behaviour.

Detective Controls

Detective controls are important components of internal controls that are implemented to identify and detect errors, inaccuracies, and fraudulent activities that have already occurred on specific transactions or business activities. Their objective is to identify any issues that remain undetected despite preventive measures and to mitigate their adverse effects. Unlike preventive controls that concentrate on preventing undesirable activities, detective controls respond to issues that have occurred. Audit trails, reconciliations, statistical analysis, and physical counts are some of the most common types of detective controls (The Institute of Internal Auditors., 2017). While detective controls may be costly, delayed, and incompatible with existing systems, they have many benefits, including detecting fraud, improving overall control, enabling management to take action, providing a basis for internal audits, and enhancing reporting integrity. Overall, the successful execution of detective controls policies and procedures helps organizations establish a robust and reliable framework that ensures the integrity of financial and operational processes. (KPMG, 2017)

Preventive Controls

Preventive controls are essential components of any comprehensive internal control system designed to mitigate an organization's risks. These controls are intended to prevent or reduce the likelihood of errors, inaccuracies, or fraudulent activities from occurring before they happen. By eliminating or reducing the possibility of these events from happening, preventive controls reduce the need to implement corrective controls after the fact. Preventive controls help organizations to comply with relevant regulations and standards such as the Sarbanes-Oxley Act (SOX), International Financial Reporting Standards (IFRS), and Generally Accepted Accounting Principles (GAAP). These regulations require that internal control systems encompass both preventive and detective controls.

In SOX, Section 404 mandates that companies establish and maintain adequate internal controls over financial reporting. This requires companies to implement preventive controls to identify areas of risk and fraud prone and to mitigate those risks/fraudulent acts before problems arise.

Corrective Controls

Corrective controls in fraud context refer to measures taken to address and respond to fraudulent activities that have already occurred. These controls are used after the detection of fraud and aim to identify the root cause of the fraud, recover lost funds or assets, and prevent the occurrence of similar fraudulent activities in the future. Corrective controls are also designed to help organizations comply with regulatory requirements and industry best practices. Many regulations and frameworks, such as the General Data Protection Regulation (GDPR) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework, require organizations to have effective controls in place to respond to security incidents. The NIST Cybersecurity Framework, for example, includes a category of controls specifically focused on responding to cybersecurity incidents (Category R) that can be used to deter fraud as procedures are amended. Corrective controls are an important part of this category, as they provide a structured and effective way for organizations to respond to incidents and meet regulatory requirements. Common types of corrective controls include restoring compromised systems, removing malware, recovering lost data, implementing investigative and behavioral controls, and changing policies and procedures. The implementation of these controls is crucial to prevent further fraudulent activities and protect the organization from financial losses and damage to its reputation. By improving fraud risk management, the implementation of corrective controls can also serve as a deterrent to future fraudsters targeting the organization.

To ensure the effectiveness of preventive controls, organizations must adhere to best practices. Firstly, conducting a risk assessment helps identify areas where preventive controls are needed, especially in potential areas of fraud, errors or control weaknesses. A comprehensive internal control framework consisting of preventive, detective and corrective controls is necessary for full coverage of fraud, errors, and other malicious activities. Controls should be reviewed and updated regularly, with the aid of internal audit department reviews, independent assessments, benchmark data from peers, and external auditor insights. Providing employee training on how to record transactions accurately, comply with policies and procedures, and report any instances of suspected fraud is crucial. Regular training sessions on how to recognize and prevent fraud can continuously help mitigate risks and maintain control awareness in the organization. Preventive controls prevent fraud, minimize errors and omissions, and reduce risk, which ensures the integrity of financial reporting and strengthens the control environment, leading to the efficient use of organizational resources.

2.5 Theoretical framework

In the research's theoretical framework, the focus will be on discussing theories related to retail fraud, specifically the Fraud Diamond Theory and the Fraud Triangle Theory.

2.5.1 Fraud Triangle Theory

Donald Cressey introduced the Fraud Triangle Theory in 1973, which suggests that trusted individuals may engage in fraudulent activities if they believe they have a financial problem that they cannot share while they have access to finances that could be secretly utilized to solve the issue. Cressey also hypothesized that there must be a motive behind any human action. The Fraud Triangle Theory comprises three key elements: opportunity, pressure, and rationalization. This can be illustrated diagrammatically below figure 1.

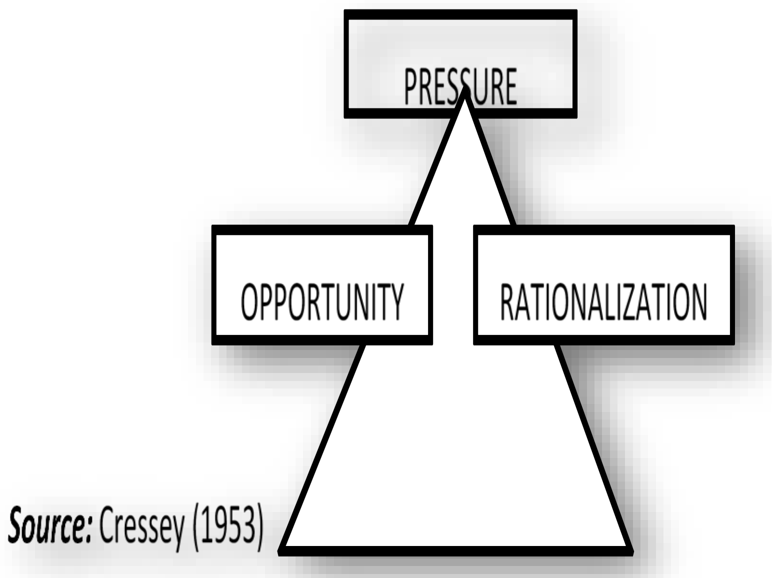


Figure 2.1 :Fraud Triangle Theory

Cressey (1953) identified three elements of fraud: pressure, opportunity, and rationalization. These elements are commonly represented in a diagram, with pressure at the top and opportunity and rationalization at the bottom (Wells 2011 in Rasha and Andrew, 2012). This is known as the Fraud Triangle Theory (FTT).

Perceived/Sensation of Pressure

The conditions that encourage unethical behavior are referred to as perceived pressure. Every fraudster is under some kind of pressure, according to Abdullahi and Mansor (2015), to act unethically. According to Albrecht et al. (2006) and Abdullahi and Mansor (2015), pressure is a crucial element in fraud, whether it takes the form of financial or non-financial pressure. It is important to note that the pressure perceived by an individual might not actually exist. Financial pressure, being one of the main types, is more likely to induce fraudulent behavior. In the retail industry, maintaining high profits may lead to vendor fraud and procurement collusion. Studies indicate that 95% of fraudulent incidents are committed due to financial pressure. Lister (2006) supports this view, stating that pressure is a primary motivator for fraudulent behavior. Furthermore, Lister (2006) identifies three distinct types of pressure that may lead to fraud: internal, external, and job-related stress. In the retail industry, suppliers may pressure an employee to commit fraud to appease them by offering kickbacks and bribes. In addition, Vona (2008) looks at corporate and individual motivations used as proxies for fraud. Some of the incentives to commit fraud include greed, living beyond one's means, significant spending or personal debt, and family financial or health issues.

According to Lister (2007), characterized the pressure for one to indulge in fraudulent activities as "the prime basis of the heat for the fire" in Abdullahi and Mansor (2015). This suggests that experiencing this pressure does not automatically lead to deception. According to Rae and Subramanian (2008), financial pressure and greed on the part of the employee is a factor in the incentive to commit fraud. Chen and Elder (2007) identified six fundamental areas for pressure a violation of an obligation, personal issues, corporate invasion, status, achievement, and interaction among workers. According to Abdullahi and Mansor's (2015) discussion of Chen and Elder's (2007) research, pressure can be divided into four categories as identified by Albrecht et al. (2008), and all of these categories are relevant to the retail industry. These categories include economic pressure, pressure related to vices, pressure related to one's job, and other forms of pressure. According to Singleton et al. (2006), these pressures are often the first step in the process of committing fraud. However, it's essential to note that this financial pressure could be symptomatic of other underlying issues that the fraudster may be facing. As such, it is crucial to take a holistic approach when identifying the root causes of fraudulent behavior. Kenyon and Tilton (2006) suggest that financial pressure or incentives can lead employees or management to commit fraud, such as accepting bribes in retail procurement.

Perceived Opportunity

Furthermore D. Cressey postulated that in the fraud triangle theory management should consider perceived opportunity, which refers to the belief that an individual has the chance to commit organizational fraud. According to Kelly and Hartley's (2010) research, having an inefficient control system creates the potential for individuals to commit fraud within an organization. Coenen (2011) notes that in the retail industry, there may be a limited number of employees, and as a result, the industry may not see the need to separate tasks. However, this can create a weak control system that provides a potential opportunity for fraud. It is important to note that for someone to commit fraud, the opportunity may not be real, but the individual must have a belief or perception that they have the opportunity. In Abdullahi and Mansor's (2015) analysis of Cressey's (1953) research, it is generally true that fraud is more likely to occur when there is a reduced chance of being discovered. Rasha and Andrew (2012), and Rae and Subramanian (2008) state that an opportunity is a flaw in the control system where the employee has the authority or capacity to take advantage of the circumstance, making fraud conceivable.

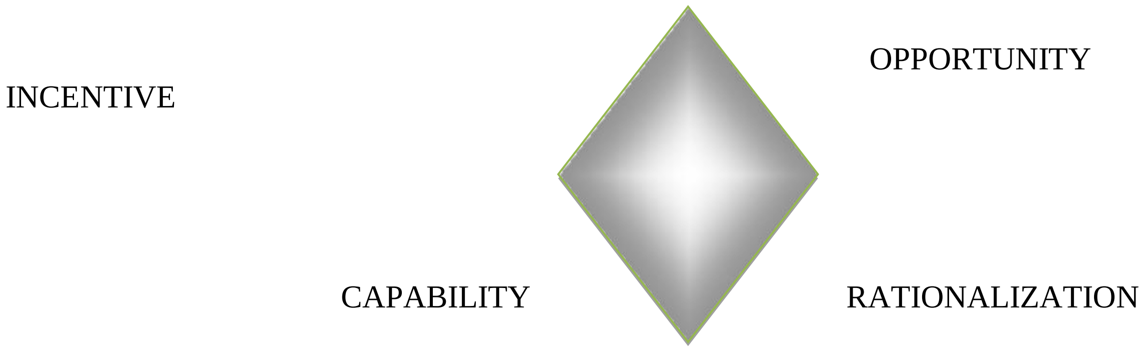
According to Hooper et al. in Abdullahi and Mansor (2015), even under conditions of intense pressure, fraud cannot happen unless an opportunity is there. According to Abdullahi and Mansor (2015), the opportunity goes hand in hand with pressure or motive since even if a person has a purpose, he cannot conduct fraud if a chance is not generated. The lack of controls or their ineffectiveness, a lack of workplace supervision, and an insufficient separation of roles, according to Kenyon and Tilton (2006), may provide possibilities for fraud. The Association Certified Fraud Examiners' (2004) Report to the Nation (RTTN) study revealed that individuals and supervisors who engage in fraud have a history of staying on the job for a long time. This is because they are aware of all the systemic flaws and have been making use of them for a long time undetected.

Rationalization

Rationalization is the third component of the Fraud Triangle Theory. According to Rae and Subramanian (2008), rationalization is the defense of dishonest action due to a worker's lack of moral character or other moral justifications. The rationalization theory contends that the offender must have a defense for their immoral action. As a result, it is argued that the person is unlikely to conduct fraud if they are unable to provide a 24 explanation. According to Cressey (1953) in Abdullahi and Mansor, rationalizations for fraudulent activity include "I was entitled to the money," particularly for workers in the retail sector who do not get a monthly salary, "I was just borrowing the money," and "I had to steal to care for my family" (2015). According to Hooper and Pornelli (2010), those who commit fraud have a certain mindset that enables them to rationalize or excuse their fraudulent behavior. Classical criminologist (Cesare Beccaria) argued that criminal action is caused as a result of free and rational decisions of acting individuals (Hidonism) that is pleasure and pain. Another theorist who supported the idea of rationalization is J Bentham who ascertained that hedonistic calculus individuals are assumed to logically weigh the benefits of a given course of action against its costs.

2.4.1 Fraud Diamond Theory

The fraud diamond theory is seen as an improved form of the fraud triangle theory, according to Abdullahi and Mansor (2015). According to Wolfe and Hermason (2004), fraud is unlikely to occur without a fourth ingredient, despite the possibility that felt pressure, opportunity, and justification might coexist. The fourth component, capacity, requires that the fraudster have the knowledge and skills necessary to carry it out. According to Wolfe and Hermason (2004), the door to fraud is opened by opportunity, and people are drawn to the entrance by incentives and rationalization but capacity permits the individual to grasp the opportunity presented by the open door and seize it. This can be illustrated below



Source: Wolfe and Hermanson (2004)

Figure 2.2: Fraud Diamond Theory

Wolfe and Hermanson (2004) argued that while opportunity creates the possibility for fraud, it is pressure and rationalization that motivate individuals to take advantage of the opportunity. Capability, on the other hand, is what allows them to recognize and repeatedly exploit the open door of opportunity.

Capability

According to Abdullahi and Mansor (2015), the capability is the circumstance where a person possesses the required characteristics, talents, or skills to conduct fraud. Position, intelligence, ego, compulsion, dishonesty, and stress are the supporting components of capacity, according to Wolfe and Hermanson (2004). According to Mackevicius and Girinas (2013), not everyone with desire, chances, and realization can commit fraud since they lack the skills necessary to carry it out or undo it. According to Abdullahi and Mansor (2015), Albrecht, Williams, and Wernz (1995) claim that capacity is particularly important when it comes to large-scale, long-term deception. Albrecht et al. (1995) assert in Abdullahi and Mansor (2015) that only a person with an extraordinarily high capacity will be able to comprehend the current internal controls, discover their weaknesses, and exploit them to plan and carry out fraud. This is particularly frequent with managers in the retail industry; they may be able to leverage the fact that stock takes only happen once a month as a way to spend some money or stock and then return it before the stock-take occurs. Wilson (2004) reveals that capacity, rationalization, and their interrelationships are all interconnected, with one factor having a bearing on the others.

Position

According to Abdullahi and Mansor (2015), a fraudster's function or position inside the organization is the first factor that provides them the opportunity to commit fraud. Cashiers in the retail sector are more prone to skim, managers to steal, and procurement officers or managers to commit procurement fraud by taking bribes or even return fraud. According to Wolfe and Hermanson (2004), an employee's role and position might influence how he develops a plan to betray the company's confidence entrusted to them.

Creativity/Intelligence and Ego

Abdullahi and Mansor (2015) suggest that fraudsters are skilled at identifying and exploiting weaknesses in an organization's internal controls, often taking advantage of their authorized access or job function. Wolfe and Hermanson (2004) argue that many major frauds in modern times are carried out by intelligent and creative individuals who possess a deep understanding of control systems and vulnerabilities. Such individuals can use their ingenuity to manipulate people into providing them with access to sensitive systems and resources. According to a study by the Association of Certified Fraud Examiners conducted in 2003, 51% of those who commit professional fraud hold at least a bachelor's degree and 49% of them are over the age of 40. In addition, managers and executives are responsible for 46% of fraud cases

Deceit, Coercion, and Stress

A cunning con artist can pressure someone into committing fraud or disguising crime (Rudewicz 2011). A charismatic individual may be able to convince others to assist in deceit or ignore it. In the retail sector, the person may be the supplier who pays off the victim's staff to choose the items, even if this degrades the quality of the final product. Wolfe and Hermanson (2004; 41) claim that a bully who "makes uncommon and substantial demands to people who work for him or her, cultivates fear rather than respect and consequently avoids being subject to the same norms and processes" may occasionally be a fraudster. Wolfe, Hermanson, and Rudewicz (2004) and (2011) assert that a successful fraudster must be a skilled liar. To avoid being discovered, the fraudster must be able to keep track of their fabrications and act consistently. One of the important characteristics of the scam is the ability to manage stress. Since it involves long-term monitoring, fraud may be quite distressing. According to Rudewicz (2011), the fraudster must have stress management skills because it may be challenging to carry out the fraud and keep it a secret.

2.4.2 Empirical Evidence

Murti and Kurniawan (2020) carried out a study on the implementation and internal control in preventing fraud using in the public sector and found out that t the weaknesses of internal control have been identified to cause fraud. Fraud will never be prevented completely, so that public sector organizations can implement internal controls to prevent and detect fraud. Management in the public sector must be able to create awareness and understanding of anti-fraud culture to all elements in the organization as an effort to prevent fraud.

Takavingofa (2017), embarked on a study of the effectiveness of internal control systems used by parastatals in Zimbabwe in reducing the risk of fraud, the main objective of her study was to ascertain the effectiveness of internal controls currently being used by parastatals in reducing fraud. Her literature review complemented that ineffective controls they create breading grounds for fraudulent activities in parastatals. The major finding of her research was that the internal controls applied were ineffective and she recommended that parastatals implement and formulate corporate fraud policies as well as bringing the concept of enterprise-wide risk management in their system.

Chikomba (2014) conducted study on the local crime risk and retail security at the Joina City Shopping Mall in Harare, Zimbabwe. According to the report, retail establishments desire an effective security program that contributes to crime reduction and prevention by implementing measures that discourage illicit conduct. Data for the study were gathered using structured and semi-structured qualitative interviews. Self-administered questionnaires and assessment interviews were also utilized to examine perceptions of security, safety, and risks associated with retail shopping. The study found that a number of variables can both raise and lower the likelihood of workplace crime. Additionally, it was indicated that a number of elements, including business location, kind of premises, customer behavior, and protective security and monitoring, have an array of various effects on crime risk. The research study went on to say in its conclusion that crime generates large losses for businesses even if there aren't any publicly available numbers on actual company loss estimates. Shoplifting, employee fraud, theft, and shrinkage are thought to be the main causes of losses for shopping mall tenants' businesses, according to the report. According to Chikomba (2014), in order to decrease fraud, retail shopping facilities need to have a strong security program. The researcher utilized this data to assess the effectiveness of internal controls in the retail sector for the objectives of the study.

A research study that was carried out by Aduam (2015) to investigate the effectiveness of internal control measures implemented in the Techiman Municipal Assembly (TMA) in Ghana. The study employed an explanatory case study research design, and the data collected was analyzed using the Statistical Package for Social Sciences (SPSS). Findings from the study revealed that the TMA does not strictly adhere to internal control procedures, which is attributed to external pressures and political interference. As a result, most public officials are not fully accountable.

In order to better understand the motivations behind and features of first-party fraud in e-tailing, Amasiatu and Shah (2014) undertook research. The authors used academic literature to outline the body of information on first-party fraud. They also examined grey literature to better understand the root causes and features of this emerging business problem. The findings revealed a variety of first-party fraud strategies and causes. According to Amasiatu and Shah (2014), compared to the recent study on the efficacy of internal controls in the retail industry, their analysis makes a case for more management attention and active participation in reducing first-party fraud.

Mishra (2006) examined two methods, internal control and random examination of employees' workspaces, that are used to deter employee theft. The study aimed to develop an inspection strategy that would save firms expenses while successfully preventing employee theft. The analytical technique employed in the study suggested that employees were strategic in their responses to the retailer's actions, and several factors - including the cost and effectiveness of random inspections and the internal control system - affected how the game played out. The study calculated the optimal inspection frequency, the total inspection expenditure, and the overall predicted retail shrinkage due to employee theft, indicating that recruiting trustworthy staff members and having a strong internal control system could assist retailers in preventing losses due to employee theft. The study's practical implications demonstrate that retailers must work to reduce inspection costs while increasing their efficacy in combating fraud in the retail sector, as addressed in the current study on the effectiveness of internal control measures.

Mugari, Gona, Maunga, and Chiyambiro conducted a study in 2016 to identify prevalent types of cybercrime in Zimbabwe's financial sector and the effectiveness of existing countermeasures. The study surveyed respondents from four commercial banks in the Harare area. The results indicated that there is a hacking problem in Zimbabwe's financial sector, with 75% of respondents acknowledging its presence. Countermeasures implemented included education and training through workshops and seminars, strict security measures, regular updates to information, communication, and technology, and the installation and constant updating of security measures like anti-virus, firewalls, and data recovery sites. The study concluded that hacking, identity theft, and harmful software usage are the most common forms of cybercrime in financial institutions. Top methods identified to reduce cybercrime include training, software upgrading, and firewalls

Mugari (2017) aimed to identify the various cyber threats that could impact Zimbabwe's retail sector and to examine the features of internet-enhanced payment systems. The study employed qualitative and quantitative research methods, using questionnaires and in-depth interview guides to collect data. The findings showed that credit/debit cards, mobile money transfers, and Real Time Gross Settlement (RTGS) transactions are the most common cyberspace-based payment methods in Zimbabwe's retail sector. The primary cyber risks facing the retail sector are virus attacks and unauthorized access, while debit card fraud and fraudulent RTGS transactions remain relatively low. Mugari (2017) concluded that despite the benefits of ICT-based payment systems, they are still prone to threats, highlighting the need for the current study's examination of internal controls in the fast-food retail sector (Quick Service Restaurant). The study also raised concerns about the inadequacy of current efforts to prevent cybercrime in the retail industry

2.5 Gap Analysis

Takavingofa (2017) conducted a study of the effectiveness of internal control systems used by parastatals in Zimbabwe in reducing the risk of fraud. The researcher conducted various thesis on the most prevalence types of frauds that affected the parastatals growth, and the most used internal controls by parastatals. In contrast this study’s pinnacle point was to evaluated the very incisive control measures that can be used to curb/minimize fraud in Simbisa Brands Quick Service Restaurants and the study also delved deep to point out the forms of retail fraud that hinder the success of any business.

Mugari (2017) conducted a study to explore the key characteristics of Zimbabwe's upgraded online payment system in the retail sector and identified various cyber threats that it faces. The emphasis was on the features of cyberspace and the risks encountered in the retail sector. In contrast, the current study assessed the effectiveness of internal controls implemented in the retail sector to prevent fraudulent activities. The research investigated the different forms of retail fraud and the preventive measures in place to mitigate them in the Quick Service Restaurants of Simbisa Brands

Chikomba (2014) conducted a study with the aim of increasing public awareness of the risks of criminal activity against businesses in Zimbabwe, and the study found that it is essential for markets to implement stringent safety measures. The present research is significant as it surveyed multiple retail outlets exclusively under Simbisa Brands and evaluated the effectiveness of the existing fraud prevention measures (internal controls).

Amasiatu and Shah (2014) conducted a study to uncover the characteristics and origins of first-party fraud in e-commerce. Through an extensive literature review, the study synthesized both current and gray literature. Along with this, the research examined the effectiveness of internal controls and the different types of retail fraud.

Muwodzeri (2019) conducted a study to examine the effectiveness of anti-fraud measures in the retail industry, specifically in the Harare CBD retail sector. The research covered supermarkets, clothing and footwear, and furniture stores. The study had a large sample size from supermarkets. On the other hand, this current study primarily focuses on the internal control systems of the fast-food retail sector, specifically in Simbisa Brands fast food outlets.

Murti and Kurniawan (2020) both conducted a study on the implementation and impact of internal controls in the public sector, to achieve these goals, researchers used a literature study of various publications related to internal control in the public sector. The authors identified poor internal controls as the grooming grounds for corruption which enhances fraudulent activities. Similarly, this research puts much synthesis on the internal controls as a way of curbing fraud in Simbisa Brands Ltd.

2.6 Summary

This chapter examined the conceptual framework that distinctly outlined the idea of retail fraud and the steps taken to prevent it. The ideas underlying retail fraud and what motivates the perpetrator to perpetrate the crime were further examined. The new investigation was then justified after taking a last look at the other studies.

CHAPTER THREE

RESEARCH METHODOLOGY

3.0 Introduction

Chapter three will explain how the research will be carried out, discussing the different methods that will be used to gather data. The focal point of this chapter will be on alleviating the research design, the target population, sample size and the sampling techniques to be applied, research instruments, validity and reliability of the instruments and data presentation and analyze the data and lastly sum up the chapter.

Research methodology sets out to define the body of practices, procedures, and rules used by those who work in a discipline or engage in an inquiry (Creswell, 2014). The other definition is the systematic, focused and orderly collection of data for the purposes of obtaining information in order to solve research questions. Research methodology it outlines the research design, data collection methods, sampling techniques, and data analysis techniques that will be used in the study (Babbie, 2017).

3.1.1 Research Design

As Nachmias and Nachmias (2012) state, a research design refers to the overall plan for conducting a study to address the research questions. According to Muwodzeri (2019), a research design constitutes the framework for collecting and analysing data. As affirmed by Babbie (2017), a research design provides the structure for carrying out research in an ethical manner.

A research design encompasses gathering evidence efficiently and in a timely fashion (Creswell, 2014). As Bryman and Bell (2015) claim, a research design offers a basis for collecting and analysing data. Therefore, the design incorporates the researcher's procedures, from formulating hypotheses to analysing data (Kothari, 1990).

A descriptive research design will be used in this study as Kothari (2004) notes that it allows the researcher to describe, analyse and report on existing conditions using both secondary and primary data. This enables the researcher to translate qualitative information into numbers for further statistical analysis and generalisation of findings from respondents (Kothari 2004).

The research design constitutes the parameters of data collection, measurement and analysis (Muwodzeri, 2019). A research design is a detailed plan for conducting an analysis or investigation. Implementing such a design allows for thorough, efficient research and maximum resource allocation.

3.1.2 Target Population/Population of the study

Generically a target population is defined as a part of a population on which the researcher would like to acquire a sample from it. Kothari (2004) postulated that a population is a group of related items or people that the researcher is eager to study. A target population equips the researcher with components /samples that can be studied to achieve a certain goal of a topic. According to Borg (2009), a target population refers to all individuals who possess certain characteristics and are of interest to the researcher. Explorable Statistics (2011) defines the target population as a large group of individuals or objects that is the primary focus of a scientific investigation. The population of a study refers to the complete set of elements or individuals that are to be examined. It represents the total number of people from which a sample is selected for the study, as explained by Blumberg et al. (2005). In this research the target population will be cashiers, accounts clerks, procurement officers, brand managers and brand accountants from the fast-food retail sector shops (Simbisa Brands) each and every brand will be selected a sample from.

3.1.3 Sample and Sampling Techniques

3.1.3.1 Sample

A sample refers to a subset of a population that is chosen and analysed to draw conclusions about the larger population (Babbie, 2016). It is a fundamental component of research as it enables researchers to collect data efficiently and economically. Random or non-random sampling techniques are used to select samples, with the sample size determined by several factors, including the research question, population variability, and available resources. To ensure the generalizability of study results, Creswell (2014) recommends that the sample accurately represents the population's demographics, behaviours, and attitudes. Even with a representative sample, there may still be some sampling error or bias, which must be accounted for when interpreting the results. In summary, samples are critical to research, and selecting an appropriate sample size and composition is crucial to the study's validity and reliability. The table below shows the sample size of the population.

Table 3.0.1 Sample size frequency

Category	Population	Percentage of population respondents
Brand Manager	**7**	**13.5**
Cashiers	**18**	**34.6**
Procurement staff	**10**	**19.2**
Accounts Clerk	**13**	**25.0**
Brand Accountants	**4**	**7.7**
Total	**52**	**100**

3.1.3.2 Sampling Techniques

According to Wilson's (2014) definition, a sampling technique is a process of selecting a smaller sample from a larger target population that shares similar characteristics with the population. The size of the sample is determined by the sampling technique employed to select the elements. Similarly, Orodho (2005) defines a sampling technique as the method used by researchers to select their samples. In this study, the researcher utilized a combination of simple random sampling and purposive sampling techniques to select the respondents. While simple random sampling entails randomly selecting elements from the population, purposive sampling involves selecting elements based on specific criteria (Babbie, 2016). The adoption of these techniques ensured that the sample was representative of the population and that the research question was effectively addressed. However, it is essential to note that the presence of sampling error and bias may still exist, necessitating their careful consideration when interpreting the study's outcomes.

Simple Random Sampling

In this case the researcher opted to using simple random sampling because it reduces/avoids the rule of biasness so that every person will get an equal chance of being selected. Simple random sampling allowed the researcher to pick respondents from different work designations and some of the employees to give their opinions regarding internal controls in Simbisa Brands at deterring fraud.

Purposive sampling

The utilization of purposive sampling technique was employed in the selection of respondents who possess knowledge and information on the implementation of internal controls in Simbisa Brands food outlets. This technique was vital in ensuring that only informed individuals from the relevant departments were selected to provide the required information concerning internal controls (Creswell, 2014). The selection of participants was based on specific criteria, such as their job title and level of expertise, to ensure that only those with relevant knowledge were included in the sample (Orodho, 2005). The combination of simple random sampling and purposive sampling techniques allowed for the selection of a representative sample that accurately reflected the population of interest.

3.1.4 Research Instruments

As per Kothari's (2004) definition, a research instrument refers to an apparatus or equipment leveraged for data collection, encompassing methodologies such as surveys, observations, and interviews. For this study, the researcher opted to employ self-administered questionnaires and interviews as the primary research instruments.

3.1.4.1 Questionnaire

As espoused by Kothari (2004), a research instrument pertains to an apparatus or contraption leveraged for data collection, such as surveys, observations, and interviews. In this study, the researcher employed self-administered questionnaires and interviews as the primary modalities for data acquisition. Moreover, as per Saunders (2003), a questionnaire denotes a meticulously curated set of inquiries devised to elicit data on a specific topic. The researcher disbursed questionnaires to all participants, excluding the brand accountants and three accounts clerks, via physical and electronic means, requesting them to peruse and comprehend the inquiries and furnish written responses on the questionnaire. Delport et al. (2011) explicate a questionnaire as a catalog of methodically structured questions that have been meticulously selected after extensive trial and error to secure dependable feedback from a targeted sample. The efficacy of questionnaires lies in their ability to elicit responses from a vast sample efficiently, given that each respondent is presented with an identical set of inquiries.

The application of questionnaires was an easy way and convenient method of conducting a survey however due to the unavailability of some co-workers at the work stations, the researcher had to avert to the use of electronic mails to reach out to all respondents. The use of electronic mails resulted in the reduction of expenses that would have alluded due to the need for printing material and transport costs to deliver the questionnaires, the emails also helped the researcher to acquire big data at a shorter time period.

The research tool employed in the present study was a meticulously structured questionnaire, as explicated by Delport et al. (2011), which served as a reliable means of eliciting responses from a targeted sample. Saunders (2003) posits that questionnaires offer an effective mechanism for collecting data from a large sample, given that each participant is presented with identical inquiries.

The questionnaire was disseminated to all the respondents in this study, affording them the opportunity to furnish written feedback regarding the pertinent subject matter. Comprised of inquiries derived from the research questions, the questionnaire's use permitted participants to deliberate on their responses, thus mitigating inaccuracies and misinterpretations (Saunders, 2003).

However, the use of questionnaires exposed the researcher to a slow start because he had to explain the questionnaires questions to the respondents for clarity's sake to those who did not understand some of the questions needs, to ensure the questionnaires were attempted, the researcher had to travel and check on respondents in different locations. Some of the questionnaires were not attempted to, hence this reduced the total amount of respondents.

3.1.4.2 Interview

Personal interviews, as elucidated by Orodho and Kombo (2002), constitute a data collection technique that facilitates a direct interaction between the researcher and the participant. This methodology entails an oral exchange of information centred on the subject matter in question. Kothari (2004) characterizes an interview as a data-gathering modality that incorporates the oral-aural transmission of stimuli and the corresponding verbal reactions. According to Orodho and Kombo (2002), interviews involve direct interaction between the researcher and the participant, with a focus on the research topic. Interviews are advantageous because they are easier to schedule and offer flexibility in the types of questions asked. Additionally, they allow for a more in-depth exploration of the respondent's thoughts and emotions regarding the research problem. Interviews like questionnaires they can get information that is accurate and free from bias since the interviewer can see the reactions and facial expressions from the interviewee.

The rate of response from the interviews was very quick and all the scheduled interviews did partake although some of the interviewees had to reschedule the meetings. The researcher was able to obtain further clarification on certain aspects through the use of interviews, which included asking follow-up questions and receiving valuable responses. The interviews consisted of more questions and answers, resulting in a wealth of useful data. The same questions from the questionnaires were further explained through the use of interviews, providing an in-depth explanation and the reasons why respondents from the questionnaires had answered so, enabling the researcher to ascertain why and grasp concepts that had been left hanging by the questionnaire.

However, some of the interviewee’s where not available at the time of meeting therefore prompting the available personnel to automatically answer on behalf of the superior hence this might have compromised the information, to those who promised to be available at a further date the researcher had to reschedule the meeting and meet up at the agreed time which made the interviews time consuming.

3.1.5 Validity and reliability

According to Zikmund (2003), the degree of reliability refers to how error-free a measure is and how consistently consistent its results are. As a result, it provides evidence of the instrument's consistency and reliability in measuring the concept and aids in determining the usefulness of a measure (Sekeran, 2006). According to Zikmund (2003), a measure's validity refers to its capacity to accurately reflect its intended purpose.

Before pilot testing, the researcher sought feedback from a panel of experts on the suitability and representativeness of the questionnaire's questions and its structure. This step improved the content validity (Mitchell, 1996:132) and enabled the researcher to make adjustments as needed. The pilot testing was conducted on a group that closely resembled the final population in the sample.

The questionnaire was pilot tested to determine the effectiveness of the wording of the questions. The researcher agreed with Bell's (1998:128) recommendation that no matter how time-constrained a researcher is, he or she must make every effort to administer the questionnaire because without a trial run, there is no way to know whether or not the questionnaire will be successful. A sufficient number of questionnaires were created, delivered personally to the respondents, and collected once they were finished. Confidentiality and anonymity were assured.

3.1.6 Data Collection Procedures

The personal interview method is an end-to-end approach that requires two people to converse, namely the interviewer and the interviewee. During face-to-face interactions, the interviewer asks questions about the subject under study. The questionnaires were personally handed out to respondents by the researcher, and data were collected from various sources using primary and secondary methods. For some of the questionnaires that were distributed electronically, the respondents received periodic email reminders, and for those that were distributed physically, the respondents also received periodic reminders prior to the date of collection. Appointments with the top management of the fast-food retail sector (Simbisa Brands) were scheduled in advance, and the interview respondents were informed or made aware of these plans. Interview responses were recorded during the interview, while questionnaire responses were gathered after they had been fully answered. Guidelines and questions to be asked were created so that the interviewee will be well vested with the parameters needed by the interviewer.

3.1.7 Data presentation, analysis and interpretation

To ensure the accuracy and clarity of the collected data, it was carefully examined and edited to eliminate any inconsistencies or inaccuracies. The data was then organized into a meaningful structure and subjected to an interpretation analysis, which involved the use of tables, pie charts, and bar charts to visually represent the data in a way that was easily understood. The quantitative data was processed using the Statistical Package for Social Science (SPSS) software, resulting in the presentation of findings in the form of tables, numbers, and percentages. This allowed for a comprehensive analysis of the data and the development of conclusions and recommendations based on the results.

3.1.8 Ethical Considerations

The ethical concerns of this study, such as ensuring informed consent, respecting anonymity, and maintaining confidentiality, were carefully considered by the researcher. Additionally, the principle of beneficence, which involves promoting the well-being of participants, was also taken into account. The researcher ensured that the respondents' privacy was respected and that the study's purpose was disclosed to them, while also obtaining permission from the relevant authorities at the retail. When a researcher is accumulating data from respondents, he or she should take into account the implications for the involvement of other personnel, with the idea of taking the least amount of risk or doing the least amount of compromise (Kumar, 2011). The researcher followed the organization's code of conduct, so respondents' information, such as their employee or worker ID number, was kept private. Additionally, some delicate information that proved to be uncomfortable was left off the questionnaires.

3.1.9 Summary

Chapter three expounded upon the research methodology utilized by the researcher to collate data from diverse sources. The chapter delved into the research design, target population, research instruments, validity and reliability, data collection procedures, data presentation, analysis and interpretation, and ethical considerations, all of which were thoroughly examined and articulated.

CHAPTER FOUR

PRESENTATION OF DATA, ANALYSIS AND INTERPRETATION

4.0 Introduction

The upcoming chapter will present the research findings extracted from the study objectives, which include determining the nature of retail fraud, identifying available internal controls in Simbisa Brands, evaluating the effectiveness of these controls, and proposing areas for improvement to reduce internal fraud in Simbisa Brands.

4.1 Profile of respondents

The profiles of the study's respondents are limited to those who completed and returned the 41 questionnaires out of the 45 that were distributed. The remaining 11 respondents who were interviewed are not included in the respondents' profile.

4.2 Response Rate of the Questionnaire (RRQ)

Table 4.0.1 Questionnaire response rate

Designation	Number of Questionnaires distributed	Number of Questionnaire responded	Response rate (%)
Cashier	14	13	92.85%
Brand Manager	6	6	100%
Accounts Clerk	12	12	100%
Procurement Officer	13	10	90.9%
Total	**45**	**41**	**91.1%**

Source: Field Data (2023)

Table 4.1 displays that the questionnaires that were distributed in the organization were 45 questionnaires to employees, out of which 41 were returned. This accounts for a response rate of 91.1%, indicating that the majority of the questionnaires were taken seriously. The profile of the respondents will focus on four primary variables: education level, working experience, age, and gender.

4.2.1 Age of respondents

The researcher analysed the age distribution of the study participants to determine the dominant age groups in Simbisa Brands food outlets. The ages of the individuals who took part in the study were grouped, and the distribution of age groups is presented in Table 4.2 for further analysis.

Table 4.0.2 Age of Respondents Table

Age	Frequency	Percent
21-25	15	28.30
26-30	8	7.55
31-35	5	15.09
36-40	3	22.64
41-44	5	16.98
45 and above	5	9.43
Population	41	100.0

Source: Field Data (2023)

According to the table above, it was found that out of the total number of respondents(individuals), 28.3% (15 individuals) were aged 21-25 years, 7.55% (4 individuals) were aged 26-30 years, 15.09% (8 individuals) were aged 31-35 years, 22.64% (12 individuals) were aged 36-40 years, 16.98% (9 individuals) were aged 41-44 years, and 9.43% (5 individuals) were aged 45 years and above.

4.2.2 Gender Distribution

Table 4.0.3 Gender Distribution

Sex	Frequency of respondents	Frequency in Percentage
Male	**28**	**67.44**

Female	**13**	**32.56**
Population Total	**41**	**100**

Primary Source (2023)

The study's results indicate that the majority of the respondents were male, accounting for 67.44%, while females made up 32.56% of the respondents.

4.2.3 Qualifications of the Population Study

Merit-based qualification (education) is primarily used to assess the abilities and knowledge of the respondents in the field under consideration. The emphasis of the study was on education as it was vital to determine the educational background of the respondents so as to determine whether they had sufficient knowledge to comprehend the effectiveness of internal control systems in the fast-food retail sector. The Table 4.4 contains the results of the study on the education level of the respondents.

Table 4.0.4 Education level of respondents

Education level	Frequency	Percent
O & A Level	19	37.40
Diploma	6	15.09
Bachelor degree	11	33.96
Master's degree	5	13.21
Total	**41**	**100.0**

Source: Field Data (2023)

Educational Level of Respondents

According to the table, the study's findings indicate that among the respondents, 15.09% held diplomas, 33.96% held first degrees, and 13.21% held master's degrees while those with O and A level qualifications made up 37.40% of the respondents.

4.2.4 Length of employment in their respective profession

The work experience of the respondents is a factor that determines their ability to comprehend issues related to the effectiveness of the internal control systems in preventing fraud in Simbisa Brands. Thus, the study provides results on the respondents' work experience which are displayed in Table 4.5

Table 4.0.5 Length (Time) of Employment

Length of employment	Total (N)number of employees	Total (N) in Percentage
3 years and below	22	50.94
4-6 years	6	22.64
7-9 years	7	15.09
10+ years	6	11.32
Total	41	100.0

Primary Source (2023)

The above table 4.5 shows that more than half (50.94%) of the respondents working in Simbisa Brands had an organizational experience of 3 years or less. Furthermore, 22.64% of the respondents had organizational experience of 4-6 years, 15.09% had organizational experience between 7-9 years, and 11.32% of the respondents had organizational experience of 10+ years.

4.3 Interview Response Rate

Table 4.0.6 Shows the Interview Response Rate

Designation	Interviews List	Completed Interviews %
Brand Accountants	4	100%
Accounts Clerks	3	100%
Cashiers	2	100%
Procurement	2	100%
Total	11	100%

Source: Field Data

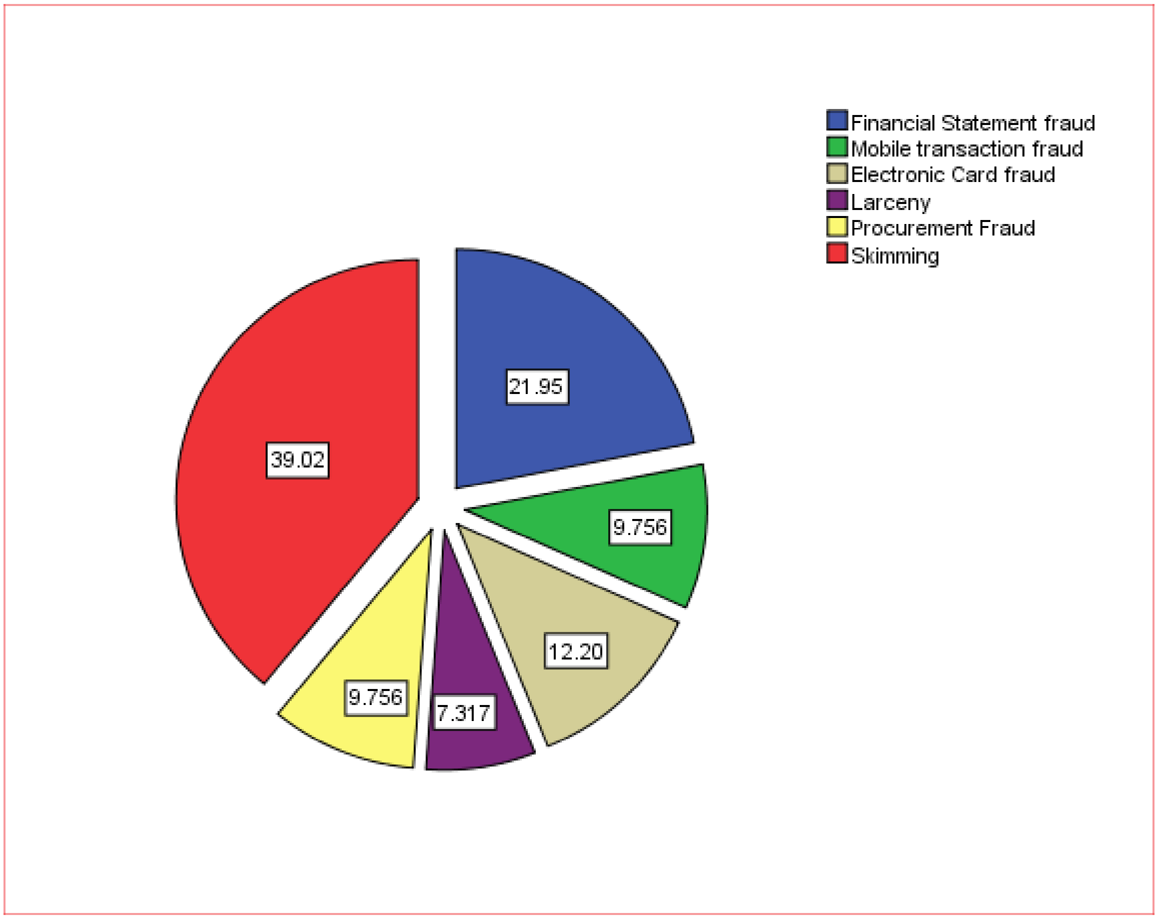
Table 4.6 shows that 11 interviews were scheduled to take place with 4 respondents being Brand Accountants and the other respondents being Accounts clerks (3), Cashiers (2) and Procurement officers were 2 in Simbisa Brands and out of the 11 interviews all of them did partake alluding to a 100% response rate.

4.4 Nature of Fraud in Simbisa Brands QSR

The participants were requested to identify the most common types of retail fraud in Simbisa Brands QSR. The data acquired from the survey provided the following outcomes.

Figure 4.1: Frequency of types of retail frauds in Simbisa Brands QSR

The pie chart below shows the views or perspectives in percentage of respondents on the ideal that there are different types of fraudulent activities occurring in Simbisa Brands retail shops.



Source: Primary data

Figure 4.3 :Types of frauds in Simbisa Brands

According to the findings of the study, the most common type of fraud that prevails in Simbisa Brands Ltd is skimming. A significant percentage of respondents, accounting for 39.02%, were aware of the fact that skimming is the most prevalent type of fraud that affects the organization. Financial statement fraud was identified as the second most common type of fraud, with 21.95% of the respondents agreeing that it occurs within the organization. Electronic card fraud had a relatively lower percentage of respondents, accounting for 12.2%, agreeing that it takes place in Simbisa Brands. Furthermore, mobile transaction fraud and procurement fraud were identified as occurring in the organization, with both types of fraud accounting for 9.756% of the respondents.

Lastly, the study found that larceny was the least common type of fraud, with only 7.317% of the respondents agreeing that it takes place in the organization.

4.5 Internal Controls in Simbisa Brands

Respondents were asked if they knew about the existence of an internal controls in Simbisa Brands Ltd.

Table 4.7 Internal Controls in Simbisa Brands Ltd

Variable	Agree	Disagree	Don't Know
Authorization	100%	0.0%	0.0%
Transaction recording	100%	0.0%	0.0%
Reconciliation	85%	0.0%	15%
Supervision	87.1%	12.9%	0.0%
Segregation of duties	91.6%	0.0%	8.4%
Reviewing payroll reports	74.6%	5%	20.4%
Internal Audits	88.8%	0.0%	11.2%
Supplier Background Check	67.8	10%	22.2%

Source: Primary source (2023)

Table 4.7 presents the results of the respondents' views on the presence of internal controls for authorization and transaction recording. The data shows that all the respondents agreed on the existence of these controls in Simbisa Brands. This means that the organization has implemented measures to ensure that only authorized individuals can perform transactions and that all transactions are recorded accurately. The respondents' agreement on the presence of these controls is a positive indication of the organization's commitment to mitigating risks and preventing fraudulent activities. In fact, all the respondents (100%) acknowledged the availability of these controls in Simbisa Brands Ltd. Additionally, 10 out of 11 interviewees confirmed the presence of these controls in the organization. The cashier and Brand Managers involved in the study also agreed on the importance of specific procedures for authorizing cash reimbursements in order to reduce the prevalence of skimming. Stamler et al. (2015) further emphasizes the significance of proper authorization in ensuring that activities are conducted by knowledgeable individuals within an appropriate range of control. They also underscore the importance of effective supervision in ensuring compliance with policies and procedures, as well as the prevention of fraudulent transactions. Moreover, transaction recording plays a crucial role in promoting accountability by identifying the nature of the transaction, who performed it, who authorized it, and when it was executed.

According to the study's findings, the vast majority of participants, accounting for 85%, engage in reconciliations as a preventative measure against fraud in Simbisa Brands. Only a minority of 15% either did not understand the meaning of reconciliations, were unaware of them, or did not perform them. Furthermore, most of the interviewees, specifically 9 out of 11, confirmed that they carry out reconciliations in their workplaces. They explained that such processes enable them to determine the amount received and the expenses incurred by Simbisa Brands. Two respondents believed that the responsibility of reconciliations lay with the top-level management. Reconciliation is an essential internal control mechanism, as emphasized by Stamler et al. (2015). The purpose of reconciliation is to verify the accuracy, completeness, and authenticity of financial information. This is in line with Wells' (2012) assertion that autonomous reconciliation and internal verification of accounts are critical general controls in the retail industry to prevent future issues. The two sources provide a cohesive and coherent argument in support of the significance of reconciliation as an internal control mechanism.

The majority of respondents (87.1%) in a study on Simbisa Brands Ltd strongly agreed on the importance of careful supervision by superiors as an internal control strategy, while a minority of 12.9% disagreed with the necessity of supervision. Stamler et al. (2015) also emphasizes the significance of adequate supervision in ensuring compliance with policies and procedures, preventing operational errors, and deterring fraudulent transactions. Additionally, the authors assert that supervision plays a crucial role in maintaining a strong control environment within an organization. To mitigate risks, management must ensure effective monitoring of personnel in carrying out their job responsibilities.

The study found that a vast majority of 91.6% of respondents acknowledged the presence of segregation of duties as an internal control mechanism in Simbisa Brands Ltd, while only 8.4% were either uninformed or unaware of its implementation. Eight of the 11 interviewees confirmed the practice of segregation of duties in the organization, while three were unaware of its implementation. Proper segregation of duties is essential to prevent retail fraud. Wells (2012) and Stamler et al. (2015) suggest that appropriate segregation of duties and access constraints can prevent fraud in ledger transactions. However, respondents noted that firms often hire a limited number of employees to reduce production costs and increase profits, which can be a challenge in segregating duties. Muwodzeri's (2019) study highlights the importance of separation of roles in avoiding losing earnings to fraudulent activities, despite increased costs or strain on the payroll. Mishra (2006) conducted research on the effectiveness of two methods (internal control and random examination of employees' workspaces) to prevent employee theft and found that retailers need to minimize inspection costs while maximizing the effectiveness of their anti-fraud measures in the retail industry. The importance of segregation of duties as an internal control measure cannot be overstated. It is crucial to ensure that there is no conflict of interest that could lead to fraudulent activities. Retailers must implement suitable segregation of duties and access constraints to prevent fraud in ledger transactions. Additionally, firms must find ways to minimize inspection costs while maximizing the effectiveness of their internal controls to reduce the risk of losing earnings to fraudulent activities.

According to the study, payroll report review is a critical internal control method that is essential for resolving irregularities in payroll systems. More than half of the respondents (74.6%) reported that they review payroll reports. Out of the 11 interviews conducted, 6 respondents acknowledged that payroll checks were done to uncover abnormalities in the payment systems. However, 5 respondents were not aware of such acts in the organization. Stamler et al. (2015) highlights the significance of conducting regular payroll reviews to minimize errors and prevent fraudulent activities. The authors suggest that payroll audits be carried out by an independent auditor to maintain impartiality. Additionally, Wells (2012) notes that payroll reviews also aid in detecting discrepancies, such as overpayment or underpayment of employees, which can be corrected before causing any problems.

Internal audits are indispensable in evaluating the efficacy of internal controls in organizations. The primary objective of internal auditing is to provide valuable insights into an organization's culture, policies, and procedures, while also bolstering board and management oversight through validating internal controls such as operational effectiveness, risk mitigation controls, and conformity with relevant laws or regulations. In the context of the study, respondents were required to indicate the occurrence of internal audits in Simbisa Brands. A vast majority of 88.8% of them confirmed that internal audits were conducted. It is important to note that organizations cannot eliminate all fraud-related issues they face. Nevertheless, the application of internal audit and internal control systems can significantly mitigate these issues, as underscored in a study by Theodoridou Paraskevi (2016). The study highlights that internal audit plays a pivotal role in monitoring and identifying risks within an organization. Moreover, Coram et al. (2006), utilizing the 2004 KPMG Fraud Survey, observed the significance of the internal audit function in detecting fraud within organizations. Thus, the existence of internal audits in Simbisa Brands is a positive indication of the organization's commitment to mitigating risks and preventing fraudulent activities.

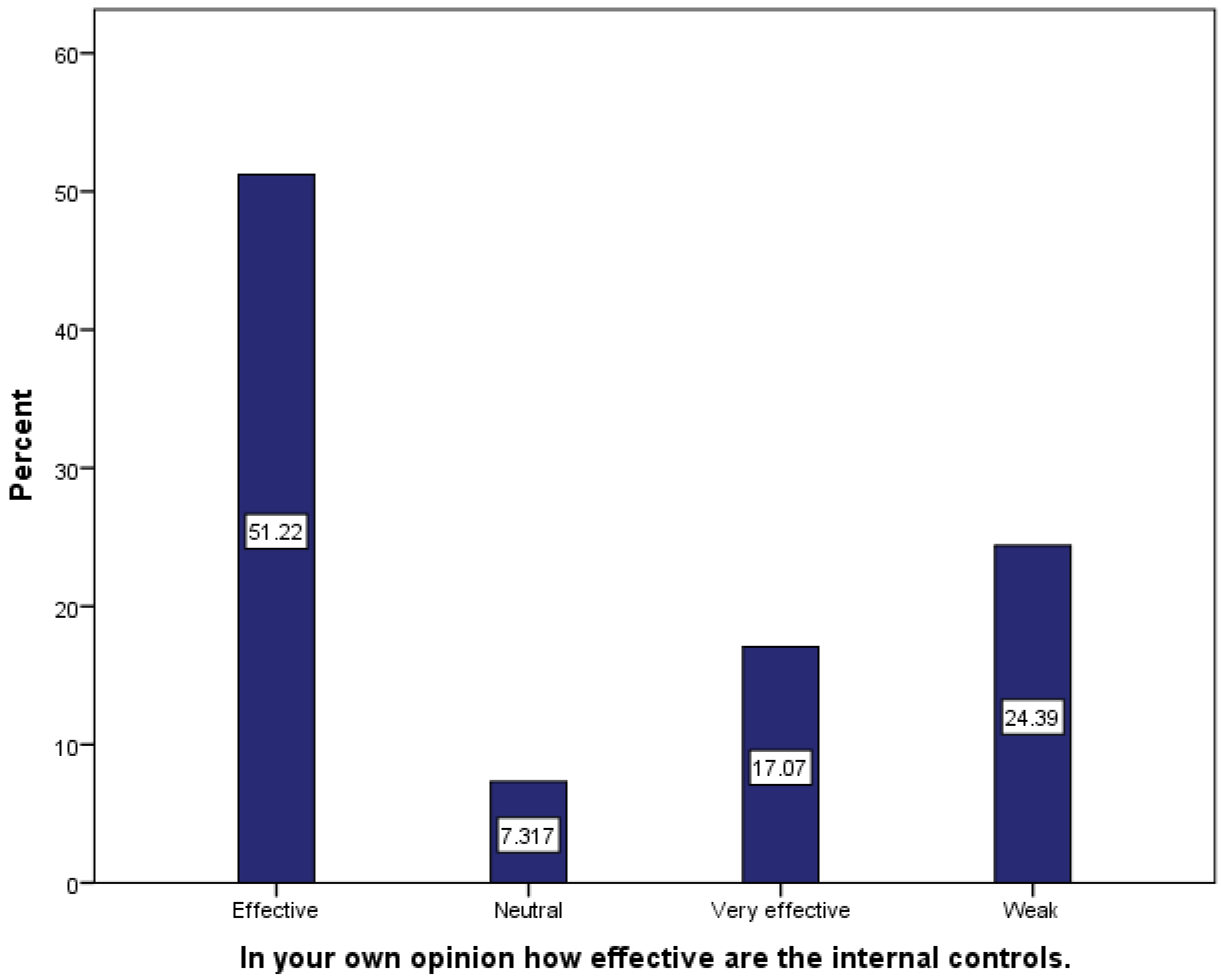
According to the study, 67.2% of the respondents conducted supplier background checks, while 10% did not and 22.2% were unsure. However, only 6 out of 11 interviewees actually performed supplier background checks. They required tax invoices, tax clearance, and certificates of incorporation from suppliers to ensure their financial stability and avoid conflicts of interest. The interviewees also emphasized the need for suppliers to have insurance to cover accidents during delivery. On the other hand, 5 interviewees did not perform background checks since they imported their goods from abroad. Nonetheless, the researcher found that larger retail organizations, such as Simbisa Brands, should conduct background checks and integrity due diligence to ensure the credibility of manufacturers. This process can reveal their interests, associations, related parties, and possible conflicts of interest. John (2003) supports this view.

The individuals who participated in the survey were asked to specify other internal controls that they employed beyond those listed on the questionnaire. The results revealed that 70% of the participants conducted stock take at the end of each month and periodically carried out spot checks. Additionally, 20% of the respondents stated that they conducted periodic spot checks and received daily work supervision from their superiors.

The results of the study revealed that 10% of the participants believed that the internal controls listed on the questionnaire were sufficient to prevent fraud. However, during the interviews, respondents confirmed that they implemented additional measures such as stock takes and periodic spot checks to minimize the occurrence of fraudulent activities. The periodic spot checks were carried out randomly without prior notice and were found to be effective in detecting fraudulent activities. For instance, one of the respondents narrated an incident where a fraudster was caught at their workstation during a spot check about a year ago. Additionally, another interviewee recalled a situation where a colleague was caught skimming during a random spot check conducted by the brand manager in October 2018, resulting in their dismissal. Therefore, periodic spot checks were identified as an effective internal control mechanism. Chikomba's (2014) study highlights that the most common crimes that cause losses in most shopping mall tenant businesses are shoplifting, employee fraud, theft, and shrinkage. To minimize these risks, it is essential to increase surveillance, engage store detectives, and use CCTV.

4.6 Ascertaining the incisiveness of internal controls in Simbisa Brands Ltd

The participants were requested to express their opinions on the efficiency of internal controls in preventing fraudulent activities. The results were presented in the form of a graph, as shown in Figure 4.3.



Source: Primary Source (2023)

Figure 4.4: Incisiveness of internal controls in Simbisa Brands

During the study, respondents were asked to evaluate the effectiveness of the internal controls in preventing fraudulent activities. Over half of the participants (51.22%) believed that the controls were effective, and a minority of 17.07% deemed them very effective. However, 24.39% of the respondents thought that the controls were weak, while 7.32% remained neutral. In the interviews, 9 out of the 11 respondents stated that the internal controls were effective to some extent, citing instances where they were able to detect and deter fraudulent activities. Although the controls helped to offer quality services to customers and protect the organization from external fraud, some respondents admitted that they could be bypassed. Two of the interviewees pointed out that the internal controls were ineffective due to the lack of separation of duties, making it difficult to identify whether workers were manipulating weak controls and covering it up. Respondents also noted that the economic hardships and corruption in Zimbabwe made the internal controls less effective. The Forensic Focus Volume 8 (2013) recommends that retailers establish a standardized plan and process for tracking, reporting, and responding to allegations of misconduct. Additionally, the investigation process should be independent of management where necessary.

During the interviews, the respondents were inquired about the regularity of introducing new internal controls and upgrading the existing ones. Interestingly, only 6 out of 11 respondents revealed that they implement these changes annually by rotating staff, particularly brand managers, across different retail outlets. However, a significant majority of 5 respondents claimed that they adhere to the existing measures unless there is a technological advancement, complaints of substandard work, or an instance of fraud. The researcher observed from the interviews that employees and managers with the longest tenure and experience are more prone to committing fraudulent activities since they have a better understanding of how the system operates. This observation is congruent with the Associated Certified Fraud Examiners' (2004) Report to The Nation, which indicates that employees and managers with extended job tenures are more likely to engage in fraudulent activities.

Some of the respondents elucidated that despite the importance of internal controls in fraud prevention and management, their implementation in Simbisa Brands fast-food industry can be challenging. One of the main challenges is the high turnover rate of employees, which can make it difficult to ensure that all employees are adequately trained in fraud prevention and detection methods. Additionally, the fast-paced nature of the industry can make it challenging to implement and enforce strict internal controls, such as segregation of duties and access controls. Another limitation is the cost of implementing and maintaining effective internal controls, which can be significant for fast-food businesses.

4.7 Recommendations

4.7.1 Recommendations Simbisa Brands Ltd

The case study respondents were requested to provide recommendations to improve the internal controls in Simbisa Brands retail sector. The majority of the respondents suggested that strict implementation of fraud management policies should be enforced, along with rigorous penalties and remedies for fraudulent activities. A few respondents proposed the availability of security cameras at their workstations and job rotation, while some respondents expressed a lack of knowledge on the matter. Based on the interviews, all respondents emphasized the need for active management involvement in upholding fraud management policy and deterring fraud. Additionally, they stressed the importance of security personnel being knowledgeable about security camera systems. Respondents without access to security cameras highlighted the need for their organizations to have them in place. Chikomba's (2014) study aligns with this view, advocating for the involvement of store detectives in CCTV usage.

Respondents also stressed out that there should be training of all employees on every induction training so that individuals will know what they are doing as procedures to ensure accountability of all actions in the organization. Mugari, Gona, Maunga, and Chiyambiro (2016) edged that companies should train their employees. Moreover, based on the interviews, the respondents emphasized the need for decentralized work responsibilities to prevent superiors from exploiting their position for personal gain. Moreover, the respondents recommended the adoption of a formalized whistle-blowing mechanism coupled with an employee assistance program to fortify the current internal control system. The incorporation of a whistle-blowing mechanism can proactively deter fraudulent activities by furnishing employees with a user-friendly, non-compulsory avenue to oversee and disclose suspected fraudulent activities. Furthermore, rewarding ethical integrity among employees is highly recommended as it could greatly enhance business operations, boost employee morale and engender a greater sense of loyalty.

4.7.2 Recommendations to the Government of Zimbabwe

Respondents stressed that the need to push for good corporate governance laws in Zimbabwe that are not ambiguous. Corporate governance is essential for ensuring the integrity, efficiency, and sustainability of businesses in different markets and contexts. It also helps to protect the interests of investors and customers, and to enhance the reputation and value of companies. The respondents who were interviewed in the study suggested that the government must prioritize the eradication of corruption as a prerequisite for successful implementation of internal controls. The respondents strongly recommended that the government impose more stringent penalties for fraudsters, thereby making the consequences of fraudulent activities more severe. This is in line with Stamler et al.'s proposal that fraud risk management guidelines include clear corrective actions and remedies for fraudulent actions. Furthermore, the study revealed that the economic recession and high inflation rates in Zimbabwe have exerted significant financial pressure on employees, which has led to an increase in fraudulent behavior. To reduce fraudulent activities in companies, the interviewed respondents recommended that the government should focus on revitalizing the country's economy by implementing measures that promote economic growth. This would alleviate the financial pressures on employees, thereby mitigating the risk of fraudulent behavior.

4.8 Summary

In this chapter, the data gathered from the research was analyzed, interpreted and discussed. The data was presented in various formats, including tables, bar graphs and pie charts. The data was collected through the use of questionnaires and interviews. The forthcoming chapter will center on the synopsis, deductions and suggestions emanating from the research.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction

This chapter includes a brief summary of the research findings, makes recommendations based on the findings, and provides an unwavering conclusion to the study.

5.1 Synopsis of the study

The primary objective of the study was to implement internal controls to manage fraud in the Quick Service Restaurant (QSR) retail sector of Simbisa Brands. The first chapter provided an in-depth account of the research background, expounded on the problem statement, elucidated the research goals and questions, and clarified the study's significance. Moreover, the chapter included the study's assumptions, delimitations, and limitations, as well as its structure. The study was steered by the objectives delineated below structure.

i. To ascertain the nature of retail fraud in by Simbisa Brands for the period 2021-2022.
ii. To identify the internal controls that are available in Simbisa Brands fast food outlets.
iii. To assess the incisiveness of the internal controls in Simbisa Brands.
iv. To propose areas where internal controls could be improved to reduce internal fraud.

The second chapter of the study was devoted to an extensive review of literature from diverse sources such as scholarly journals, books, and newspapers. This chapter comprehensively covered the conceptual framework, theoretical literature, and empirical evidence that informed the study. The third chapter, however, primarily concentrated on the research methodology, encompassing facets such as research design, population of the study, sample size, sampling techniques, research instruments, data collection, presentation, and analysis procedures. These procedures were meticulously outlined to ensure that the research adhered to rigorous scientific standards.

5.2 Synopsis of research findings

The researcher found out that skimming was the most predominant type of fraud that was being perpetrated in Simbisa Brands Ltd followed by financial statement fraud and electronic card fraud respectively the reason behind being that skimming does not raise much alarms, the employer will need much time to ascertain that fraudulent activities are taking place. Electronic Card fraud was found to be the 3rd most predominant type of fraud, with a lot of respondents mentioning that this kind of fraud was on the rise due to the increase in technology of internet banking when fraudsters use technology to steal information of an individual's account. Some of the respondents explained that as technology advances and more transactions move to electronic payment systems, criminals are finding new ways to steal payment card information. This includes tactics such as skimming, phishing, and hacking. Additionally, with the COVID-19 pandemic in 2019 led to an increase in online shopping, there has been a corresponding rise in card-not-present fraud. Lack of awareness and education among individuals and businesses about how to prevent card fraud is also a contributing factor.

According to the research conducted, the majority of respondents were satisfied with the internal controls in place in Simbisa Brands, such as authorization, transaction recording, and segregation of duties. However, a significant number of respondents found these controls to be inadequate and ineffective in preventing retail fraud. This indicates that there is still room for improvement in the management of fraud risks in the retail sector. The study also revealed that corruption has weakened the justice system, thus rendering the internal control laws in Zimbabwe less effective. Therefore, it is recommended that the government take a more active role in combating retail fraud by implementing stricter penalties for offenders and raising awareness on the issue of corruption. The management of Simbisa Brands is urged to actively participate in the implementation and monitoring of effective fraud management policies to minimize the risk of fraud in their retail sector.

5.3 Conclusion

In conclusion, the researcher's findings suggest that fraud is a significant issue in Simbisa Brands' retail sector. The researcher identified several types of fraud, including skimming, financial statement fraud, and electronic card fraud. However, the study also revealed that the company has implemented internal controls to address this issue. Specifically, Simbisa Brands commonly uses authorization, documentation, and reconciliation to minimize fraud. While the majority of respondents indicated that they found these measures effective, a few were dissatisfied with the internal controls at their organizations and found them to be ineffective. Despite the presence of internal controls, the researcher recommends that more effort is needed to make them even more effective. This involves active participation from important key stakeholders in the company to ensure that the internal controls are implemented and monitored effectively. Additionally, the study suggests that active involvement in the implementation of risk management and laws can be effective in curbing retail fraud. It is clear that there is a need for a holistic approach to fraud prevention, involving both internal controls and external measures, to ensure the integrity of Simbisa Brands' retail sector.

5.4 Recommendations

Engagement of stakeholders.

Based on the aforementioned findings, it is advised that the retail industry take the issue of fraud risk seriously. The establishment and implementation of internal controls should be treated with utmost importance, and all parties involved should be engaged in the development and monitoring of the fraud risk management policy. The first recommendation suggests that employees in the retail sector should receive regular training to increase their awareness of internal control procedures. This could involve educating employees on how to identify fraudulent activities and reporting them in a timely manner to prevent financial losses.

Management Active Involvement

The management should be active in their workplaces, when implementing the fraud risk management policy. It is recommended that they strictly assess and monitor the work policies in conjunction with the risk management policy. The management should also make sure everyone is aware of these policies to avoid complications. They should spear head and lead by example.

Government active involvement

The study suggests that the government should take an active role in the retail sector to prevent retail fraud. One way to achieve this is by increasing penalties for those found guilty of committing retail fraud. Furthermore, the government can raise awareness about corruption and the weak justice system, thereby strengthening the fight against retail fraud. The researcher also recommends that the government should launch active campaigns to prevent crime.

Strengthening the Collusion Prevention Mechanism

The third recommendation is directed towards strengthening the collusion prevention mechanism by separating duties. This involves ensuring that no single employee has control over an entire process, such as purchasing, billing, and payments. By separating duties, the risk of an employee colluding with others to commit fraud is reduced, since it would require the involvement of multiple individuals to carry out a fraudulent activity. This approach aims to create a system of checks and balances, preventing fraudulent activities from occurring.

Continuous Work Assessment

It is recommended that retailers continuously update and improve their fraud risk management policies. The researcher believes that keeping up with the latest technology, particularly in the context of e-commerce, is crucial for businesses to stay competitive and meet consumer tastes and preferences.

5.5 Recommendations for future research

The study recommends further study on the effectiveness of cyber security in curbing fraudulent activities in the retail sector. The study will have to focus on how cyber security can be used to deter fraud by organizations since the advancement of technology has been associated with an increase fraudulent activity being perpetrated by individuals through the use of computers or computer aiding.

REFERENCES

Abiola, I. & Oyewole, A. T., 2013. Internal control system on fraud dtection: Nigeria Experience. *Journal of Accounting and Finance* , 13(2013), pp. 141-152.

Accountancy Europe, 2019. *Accountancy Europe.* [Online]
Available at: https://www.accountancyeurope.eu/wp-content/uploads/190513_Tax-Policy Update_Accountancy-Europe
[Accessed 01 April 2023].

Action Fraud, 2023. *National Fraud and Cyber Crime Reporting Centre.* [Online]
Available at: https://www.actionfraud.police.uk/a-z-of-fraud/asset-misappropriation-fraud#:~:text=It%20can%20also%20be%20known,and%20interests%20of%20an%20organisation.
[Accessed 21 April 2023].

Babbie, E., 2017. *The practice of social media research.* 14 ed. Belmont: Wadsworth.

Barra, R. A., 2010. The impact of internal controls and penalties on fraud. *Journal of Information Systems,* 24(1), pp. 1-21.

Cornell Law School, 2021. *Legal Information Institute.* [Online]
Available at: www.law.cornell.edu/wex/larceny.
[Accessed 25 04 2023].

Creswell, J. W., 2014. *Research Design:Qualitative,quantitativeand mixed methods approaches.* 4th ed. Thousand Oaks,CA: Sage.

Ernst and Young, 2009. *Ernst and Young.* [Online]
Available at: https://www.ey.com
[Accessed 26 04 2023].

Kothari, R., 2004. *Research Methodology Methods and Techniques.* 2nd Edition ed. New Delhi: New Age.

KPMG, 2017. *KPMG.* [Online]
Available at: https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/08/internal-control-a-practical-guide.pdf
[Accessed 22 10 2022].

Kumar, R., 2011. *Research Methodology a Step by Step Guide for Beginners.* 3rd ed. s.l.:Sage.

Merriam-Webster, 2021. *Merriam-Webster.* [Online]
Available at: legal-dictionary.thefreedictionary.com/Larceny.
[Accessed 25 4 2023].

Nachimias, C. F. & Nachimias, D., 1996. *Research Methods in Social Sciences.* 5th ed. London: Anorld.

Pathlock Team, 2021. *Pathlock.* [Online]
Available at: https://pathlock.com/learn/internal-control-framework-a-practical-guide-to-the-coso-framework/
[Accessed 30 March 2023].

Posey, B., 2023. *TechTarget.* [Online]
Available at: https://www.techtarget.com/searchcio/definition/COSO-Framework#:~:text=The%20COSO%20Framework%20is%20a,accordance%20with%20established%20industry%20standards.
[Accessed 30 March 2023].

Rae, K. & Subramaniam, N., 2008. Quality of internal control procedures. *Managerial Auditing Journal,* 23(2008), p. 124.

Saunders, M., 2003. *Research Methods for Business Students.* 2nd ed. New York: Prentice Hall..

Saunders, M., Phillip, L. & Adrian, T., 2015. *Research methods for business students.* 7th ed. Edinburgh gate, Harlow, Essex CM20 2JE, England: Pearson Education Limited.

Schneider Wallace Cottrell Konecky, 2023. *Wallace.* [Online]
Available at: https://www.schneiderwallace.com/practice-areas/whistleblower-

claims/procurement-fraud/examples-of-procurement-fraud/
[Accessed 16 03 2023].

Study.com, 2023. *Study.com.* [Online]
Available at: Study.com, Study.com, study.com/academy/lesson/what-are-preventive-controls-definition-examples.html.
[Accessed 23 4 2023].

The Balance, 2021. *The Balanace Small Business.* [Online]
Available at: http://www.thebalancesmb.com/controls-detective-corrective-and-preventive-397877
[Accessed 23 04 2023].

The Institute of Internal Auditors., 2017. *Internal Audit's Role in Detecting Fraud.* [Online]
Available at: http://www.theiia.org/download.cfm?file=25135
[Accessed 28 4 2023].

The Sunday Mail, 2023. *Confronting fraud, theft in companies.* [Online]
Available at: https://www.sundaymail.co.zw/confronting-fraud-theft-in-companies
[Accessed 23 05 2023].

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

Wells, J. T., 2011. *Corporate fraud handbook: Prevention and Detection.* 3rd ed. Hoboken, New Jersey: John Wiley and Sons.

Wolfe, D. & Hermanson, D. R., 2004. The fraud Diomond. *Considering the four elements of fraud,* 3(12), p. 74.

Zikmund, W. G., 2003. *Business Research Methods.* 7th ed. New York: Thomson Learning.

The Basel Committee on Banking Supervision. (2011). Basel III: A global regulatory framework for more resilient banks and banking systems. https://www.bis.org/publ/bcbs189.htm

The European Banking Authority. (2018). Guidelines on fraud reporting under the Payment Services Directive 2 (PSD2). https://eba.europa.eu/sites/default/documents/files/document_library/Guidelines/2018/GL_on_fraud_reporting_under_PSD2.pdf

The Financial Stability Board. (2014). Guidance on Supervisory Interaction with Financial Institutions on Risk Culture. https://www.fsb.org/wp-content/uploads/r_141118.pdf

The International Organization of Securities Commissions. (2018). Principles for the regulation and supervision of commodity derivatives markets. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD591.pdf

APPENDICES

APPENDIX 1: RESEARCH ASSISTANCE LETTER AND QUESTIONNAIRE

Bindura University of Science Education

Private bag 1020

Bindura

To Whom It May Concern

Dear Sir/Madam

RE: Request for Research Assistance

I am Chamboko Prince, a Financial Intelligence student at Bindura University of Science Education, currently carrying out a scholarly research study on **"Managing Fraud using Internal Controls: A Case Study of Simbisa Brands Fast Food Retail Sector from 2021-2022".**

This survey is a mandatory component in the process of obtaining a Bachelor of Commerce Honor's Degree in Financial Intelligence. Its aim is to investigate the type of fraud occurring in the fast-food retail industry, the existing internal controls that aid in preventing, detecting and deterring fraudulent activities.

Your voluntary participation in completing the questionnaire is much appreciated, and you have the option or freedom to opt-out of the research or study at any point in time without facing any adverse consequences or implications. Please be assured that all responses will be kept confidential and utilized solely for research purposes.

I highly appreciate your willingness to take part in this study

Instructions

Complete in ink.

Kindly respond to the questions in this survey by ticking the boxes or filling the spaces where necessary. Avoid writing your name on any of the pages comprising the questionnaire.

Questionnaire

Section A

1. Kindly specify your gender.

☐ Male ☐ Female

2. Please specify your age group.

☐ 21-25 years ☐ 26-30 years ☐ 31-35 years ☐ 36-40 years ☐ 41-44 years ☐ 45 years and Above

3. Duration of employment

☐ 3 years and below ☐ 4-6 years ☐ 7-9 years ☐ 10 years and above

4. Employment category

☐ Brand Manager ☐ Procurement Officer ☐ Cashier ☐ Accounts Clerk

5. Level of Education
   a) O & A Level
   b) Diploma
   c) Bachelor's Degree
   d) Master's Degree

Section B

6. Which types of fraud are frequently encountered in Simbisa Brands Ltd? Please mark the ones that apply by ticking the box(es).

Nature of fraud	Yes	No
Electronic Card fraud		
Procurement Fraud		
Skimming		
Larceny		
Mobile transaction fraud		
Financial Statement fraud		
Other		

7. Are there any additional types of retail fraud that are common in Simbisa Brands fast food retails? If yes, kindly specify them in the spaces provided.

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

Section C

8. What internal controls are in place to reduce or prevent instances of fraud in Simbisa Brands Ltd?

Control Activities	I Agree	I Disagree
Reviewing Payroll reports		
Transaction recording		
Reconciliations		
Authentication		
Supervision		
Segregation of duties		
Internal audits		
Supplier background check		

9. Does Simbisa Brands have a Risk Management department?

☐YES ☐NO ☐DON'T KNOW

Section D

10. Can you express your level of satisfaction with the internal controls currently present in Simbisa Brands Ltd on a scale of 1-5?

Level of Satisfaction	**1**	**2**	**3**	**4**	**5**
Tick here					

11. In your own opinion how effective are the internal controls.

Variable	Very Weak	Weak	Effective	Very Effective
Segregation of duties				

Authentication				
Physical Controls				
Employee screening and training				
Internal Audits				
Reconciliations				
Payroll reviews				

12. In your view, how effective are the internal control regulations in Zimbabwe in preventing retail fraud? Please provide your response below.

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

Section E

13. What measures do you suggest to enhance the internal control procedures in your organization in order to effectively prevent fraud?

……………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

End of questionnaire

Thank you for your co-operation

APPENDIX 2: INTERVIEW GUIDE

Interview Guide

3 Interview questions

1. What types of fraudulent activities impact Simbisa Brands QSR?

2. Have you reported any fraud to authorities and if so, how was it handled?

3. What are the consequences of fraud in your organization?

4. What internal controls are currently in place?

5. How knowledgeable are employees about these controls?

6. How effective have these controls been in preventing fraud?

7. How often are internal controls reviewed and updated?

8. How effective do you think internal controls are in preventing fraud in the retail sector?

9. What recommendations do you have to improve internal controls in your organization?

10. What measures do you suggest the government take to enhance internal controls and prevent fraud in the retail sector, in your opinion?