EXPLORING THE IMPACT OF ANTI-FRAUD CONTROLS

ON OCCUPATIONAL FRAUD

by

Gunjan Jain

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

In Partial Fulfillment

Of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

January, 2025

EXPLORING THE IMPACT OF ANTI-FRAUD CONTROLS ON OCCUPATIONAL FRAUD

by

Gunjan Jain

Supervised by

Dr.sc. Hrvoje Volarević

APPROVED BY

____

Dissertation chair

RECEIVED/APPROVED BY:

____

Admissions Director

Dedication

This thesis is dedicated to my parents, Mr. Arun Kumar Jain and Mrs. Jaishri Jain, who have been my greatest supporters throughout my life. Your love, wisdom, and tireless belief in me have made me who I am today. This achievement is as much yours as it is mine.

To my friends, Devyash and Suvidhi, thank you for your friendship, encouragement, and for always reminding me to keep going, even when things felt impossible. You helped me through the toughest times, and for that, I will be forever grateful.

Finally, I dedicate this work to all those who have faced challenges along the way but never gave up. Your perseverance and resilience inspire me every day.

Acknowledgements

Completing this thesis has been a long and challenging journey, and I could not have done it without the help and support of so many wonderful people.

First, I would like to thank my supervisor, Dr.sc. Hrvoje Volarević. Your patience, expertise, and unwavering belief in my potential have made all the difference. You not only guided me academically but also inspired me to think critically and pursue my research with passion. Your advice has been a constant source of motivation.

I am also incredibly grateful to the members of my thesis committee.

To my parents, Mr. Arun Kumar Jain and Mrs. Jaishri Jain, words cannot express how thankful I am for your love and support. From day one, you believed in me, even when I had doubts about myself. Your sacrifices and constant encouragement have been my rock. This accomplishment is as much yours as it is mine.

I also want to thank my friends and colleagues who made this journey less lonely. A special thanks to Mr. Devyash and Ms. Suvidhi for the countless hours of brainstorming, discussing ideas, and offering words of encouragement when things got tough. You have been my sounding boards, my motivators, and my comforters.

To everyone who has contributed to this research, whether through direct help or simply by being there when I needed it most, I am deeply grateful. This thesis would not have been possible without your support.

ABSTRACT

EXPLORING THE IMPACT OF ANTI-FRAUD CONTROLS ON OCCUPATIONAL FRAUD

This dissertation focuses on adaptation to anti-fraud controls in view of changes in business conditions, namely those brought upon by the virus commonly known as COVID-19. Again, after the pandemic, the efficacy of anti-fraud mechanisms or systems within different departments at an organizational, business, and sectoral level of occupational fraud within an organization comes into question. Of interest to the study at hand is also the identification of areas where changes have been affected and examining the effectiveness they have had while attempting to control cases of occupational fraud.

This study embraces a mixed-methods approach through quantitative and qualitative survey to garner responses across different industries. It considers the various specific anti-fraud strategies for different departments, such as HR, Finance, Operations, and IT, besides sectoral and organizational size differences. Some major themes in these measures range from traditional ones involving internal controls and audits to modern techniques of AI, machine learning, and data analytics.

The results show that organizations with a full anti-fraud framework tend to report fewer fraud incidents, emphasizing proactive steps like employee training, strong internal controls, and real-time data monitoring. Similarly, the adaptation to enhanced cyber security protocols, remote fraud monitoring tools, and better coordination between departments since the pandemic was partial across different departments and sectors. Large organizations had advanced systems, while SMEs faced resource allocation challenges and difficulties in integrating technology.

The study concludes that even though traditional anti-fraud measures are still relevant, integration of innovative technological solutions and frequent training among employees is hugely required in the fight against contemporary fraud risks. Additionally, instilling a culture of ethical accountability and increasing inter-agency collaboration will go a long way toward strengthening organizational resilience against occupational fraud. It is a study adding to existing knowledge through actionable insights in the direction of anti-fraud strategies and thus provides a framework from which organizations can adapt measures to suit their needs and specific vulnerabilities. This dissertation underlines the dynamic character of fraud prevention and accordingly proposes adaptive strategies for mitigating occupational fraud in a world where business is becoming increasingly complex and digitalized.

Gunjan Jain

2025

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I: INTRODUCTION

1.1 Research Background

The number of new cases of such fraud revealed worldwide has exceeded 2,690, and the total loss from them is more than 7 billion $. According to the bill for job fraud and abuse of powers in the Middle East, they have surpassed those in the world. In the report United Nations: Job Fraud and Abuse of Job Powers AA issued that in the Middle East, the average cases of fraud and job power are 200000$ which is the second highest in the world, and the cases studied in 2020 by Abu Amuna.

Almost all surveys carried out by large accounting and consulting firms show that fraud is a worsening problem for organizations across the globe. Fraud-fighting programs comprise policies, procedures, and techniques designed for management use. Based on specialized works of the World Bank, the internal control system that a sound control environment can be achieved is the internal control for public sector organizations to reduce the risk of fraud, Moreover, the strong monitoring system for Fraud does not ensure that the organization will not take place, so other defense lines including internal and external audit system and other additional systems need to be established. Bhargava, (2024).

In a survey on fraud conducted by ACFE, it was reported that the government sector came second in representation. Fraud practices follow in the steps of the banking sector as well as other financial institutions. The study also revealed that the size of the organization is directly proportional to the rate of fraud. The study also revealed that fraud can easily and mostly be committed in the public sector organizations. Other research shows that about 60% of companies in America have experienced fraud and that sound organizations experience a loss of 5 percent as a minimum to fraud and financial corruption. A survey of Palestinian citizens conducted by AMAN Foundation in 2018 on the nature and combating fraud in Palestine revealed that the most critical issues that need to be addressed to solve it is the problem of fraud. Thus, the figures show that the percentage of citizens who considered the existing efforts to combat fraud to be insufficient in 2018 has also grown although the efforts to combat fraud are still weak and inadequate Bhargava et al., (2020).

The problem of fraud is still actively developing in worldwide logistic organizations. The number of new cases of identified fraud exceeds 2690, and their total cost – is 7 billion Iriqat et al., (2020). The Middle East area has been highly affected, with average cases of fraud and abuse of power Dud for two hundred Thousand only second in the world as per data from the United Nations (UN) 2018. According to the Association of Certified Fraud Examiners (ACFE), the government area occupies the second position in terms of the number of fraud reports, while the banking and other financial organizations are closely followed Iriqat, (2020). Both the Department of Auditor General and the World Bank Group have highlighted the internal control system as a powerful tool in the minimization of fraud, more so in government organizations Bhargava, (2020). Proper control of sound, an internal and external audit system, and other additional systems are key defensive barriers against fraud. Thus, even with the high effectiveness of monitoring and control, fraud risk cannot be excluded completely, which proves the necessity of using a multiple approach to fraud risk management.

Available literature also reveals that fraud frequency increases with firm size because as the size increases, the rate of fraud rises Khaksar et al., (2020). Additionally, a study done on different firms in America discovered that nearly 60% of firms had been hit by fraud, for sound firms, fraud and financial fraud had caused a minimum of 5% loss Hilal et al., (2022).

A study undertaken by the AMAN Foundation in Palestine in 2018 shows that while researching the nature and the fight against fraud, the challenges that have to be met to solve the problem of fraud are the insufficient attempts to prevent fraud and the inefficiency of the attempts being made Abu Amuna et al., (2020). The survey also indicated that the percentage of the citizens noticing the previous measures as inadequate has increased over time which means that there is a strong need to enforce more effective methods for preventing fraud and detecting it.

From the research carried out in this paper, the rising trend in corporate deception coincides with the introduction of the digital age. The conventional forms of fraud are as listed below fundamentals, embezzlement of funds or stock, bribery, and corruption, regulatory fraud, procurement fraud, money laundering, MA fraud, financial wrongdoing, capital market fraud, and fraudulent conversion of assets Ogbomo, et al., (2020). However, there are some new types of fraud caused by technological development these years, such as counterfeiting fraud, cloud computing fraud, social media fraud, e-commerce fraud, and Cryptocurrency fraud Anderson et al., (2019). Telecommunication fraud has not been left behind on fraudulent activities, it includes network fraud, invoicing fraud, CRM fraud, financial system fraud, and procurement fraud Ahmad et al., (2020). Babaei et al., (2019) stated that traditional telecommunications fraud can be categorized into four broad categories: Legal fraud, contractual fraud, technical fraud, procedural fraud, and hacking fraud. He has categorized mobile fraud into the following categories: subscription, direct inward system access, PBX hacking, call selling or phony traffic, revenue share, payphone traffic, bypass and occupational fraud or dealer/sales fraud, packet splitting, an unauthorized credit adjustment, voucher fraud, leakage of credit card data, and selling of billing information. Organizational fraud risk is especially high largely because occupational fraud is a practice committed by organizational insiders who are directly controlling or implementing organizational activities. There has been a three-fold increase in internet users from 1,596 million users in March 2009 to 4,536 million users in June 2019 since the launch of 4G LTE technology in 2009 Ahmad et al., (2020).

Global mobile internet user penetration was projected to reach approximately 3.5 billion users in 2019 according to the GSMA. This means it approximates, or likely represents about 50 percent of the global population, using mobile data Mache, (2023). Mehta et al., 2024 reported that smartphones account for 52.2% of internet usage globally, and this is rising elsewhere. This market has been growing phenomenally, three times faster than traditional retail shops. However, the phenomenal growth in mobile internet usage is expected to shift m-commerce as the model for e-commerce consumption in daily life. This has led to the birth of a new level of fraud, which is more dangerous for data protection and security taking into account the increasing numbers of mobile banking, e-commerce, IoT third-party services, etc. Ahmad et al., (2020).

This question has also been made relevant by the COVID-19 pandemic, which has enhanced more and more remote work and digital transactions, creating new opportunities for fraudsters to take advantage of existing gaps in organizations' fraud control systems and procedures Klapper et al., (2021). There has also been growth in the use of technological solutions in combating fraud during and after the pandemic, though the efficiency has not yet been ascertained.

In recent years, bad practices have also become increasingly evident in public sector organizations, which can also be a target for fraudulent activities Naher et al., (2020). The study has identified that public sector organizations are most vulnerable to fraud due to poorly developed or nonexistent internal controls and high levels of operational complexity.

Based on such findings, there is a need to assess the present level of protective steps concerning fraud in organizations, especially after the outbreak of COVID-19. This present study has the purpose of adding to the existing literature on fraud prevention and detection to assess existing strategies and to determine the best practices for fraud prevention and detection in organizations Kennedy et al., (2021).

The banking institution is very prone to insider threats within the financial system and therefore demands specialty in risk management measures due to unarguable social cost when buckling. For instance, by the authorities of the USA during 2008-2011, 355 initial commercial banks and 57 savings and loan associations were declared insolvent and shut down. These failures will have cost up to $90 billion to the economy Singh, (2013). Furthermore, there are many cases worldwide of internal weaknesses or threats to the financial sector. There are 361 cases of employee embezzlement in Korean commercial banks, insurance, and securities companies in the five years from 2010 to 2014. The total loss of the employee embezzlement cases was executed at £103 million Valiquette L'Heureux, (2020). Former derivatives trader Nick Leeson brought Barings Bank in the UK to its knees through fraud and the bank lost £850 million Goldberg, (2012). Against this backdrop, Jerome Kerviel, a trader at Société Générale lost about £4 billion and was charged with forgery, trafficking of forged documents, unauthorized use of the computer, and breach of trust. Worldwide, fraud and corruption in financial institutions are some of the root causes of serious banking crises including; Savings & Loan Debacle, and Subprime Mortgage Crisis. Youvan et al., (2024).

Within the white-collar criminology arena, Donald Cressey's Fraud Triangle proposed that three interrelated elements must be present for someone to commit fraud: The rationale for the fraud, the incentive or pressure which creates a desire in a person to perpetrate the fraud, the chance or the possibility through which the fraud can be carried out and the capacity of the fraudster, before he or she goes ahead to perpetrate the fraud, to justify the fraud Ehigie Aimienrovbiye Humphrey, (2024). According to many previous works, one of the most consistent predictors of fraud is timing, which indicates that sufficient internal controls are not available as they offer an opportunity to perpetrate fraud Bonrath et al., (2024).

1.1.1 Fraud Prevention Techniques: An Overview

Fraud prevention is one of the most important segments of organizational management that inevitably implies the utilization of specific measures and approaches to prevent fraud, recognize it, and meet the essential corresponding activities. Fraud control measures are put in place because occupational fraud is a threat that poses varying levels of losses and damages to organizational reputations Musyoki, (2023). These mechanisms can be categorized into three main types: Preliminary, surveillance, and correct control. Most preventive controls are designed specifically to avoid the occurrence of fraud within a company, while detective controls are designed to detect the occurrence of fraud, and corrective controls are designed to rectify the effects of fraud Hameed et al., (2019).

In an organizational view, fraud prevention is important because it safeguards organizational assets, builds stakeholder confidence, and complies with the law. It also shows that with proper approach and accurate fraud prevention mechanisms can be useful to organizations to minimize the opportunities for fraud, increase their credibility, and boost overall functionality. This paper shows that as technology advances, the techniques used by fraudsters also advance. They are always coming up with new tactics of defrauding systems and exploiting every form of what is currently existing in real-time actions. In exercising this right, organizations are required to be offensive to remain secure, eradicating any doubt or hesitation that hampers innovation. They cannot only wait for something to go wrong and then pull their acts for the fix; they have to act proactively Bello et al., (2024).

These fraud detection techniques save companies from losing money and people's private information while ensuring everyone trusts the business. In a world where fraud can occur in very intelligent ways, any organization needs to have a strategy on how to avoid such incidents in the current technological world. Detected preliminary controls include measures taken to minimize the chances of fraud occurrence Kenyo et al., (2012). These consist of measures like; screening of employees, keeping operations in distinct departments separate from one another, and approvals. Surveillance controls, on the other hand, are measures and control mechanisms that are supposed to detect fraud as it takes place. Some of the surveillance controls are periodic, records or transaction processing, and evaluation of financial statements. Detective controls' goal is to fix the consequences of fraud that has already taken place. Such controls comprise disciplinary measures, compensational measures, and measures to recover loss Baba, (2019).

Other controls that organizations can use include the various fraud-fighting measures that can be used to detect fraud. This is according to the Association of Certified Fraud Examiners (ACFE), where we find that having awareness of such controls deters fraud in the best way possible Courtois et al., (2020). These strategies should nonetheless be checked from time to time and modified as required to be productive.

That is why fraud prevention is necessary as it protects organizational resources, increases shareholders' trust, and meets legal requirements. By having good methods and relevant anti-fraud measures, fraud risks are reduced to the lowest level and companies' credibility, as well as functionality, improve.

- **Fraud Prevention versus Fraud Detection**

Fraud prevention includes all the measures the organization has in place to prevent fraud. On the other hand, fraud prevention is conducting observations of transactions and customer's behavior to prevent fraudulent actions after they have been committed Rashid et al., (2022). These strategies are symbiotic: one, detection deals with a threat that is already identified, while prevention protects from possible threats that make it more difficult for the criminal to thrive in fraud.

- **Internal Controls**

A close examination of Cohen reveals that internal controls act as an important preventive measure against fraud risk. Various risk audits carried out by several parties within the organization, and even external auditors, increase the prospects of fraud prevention and detection as well as fraud investigations. Another element of controls also should be reviewed and modified more often or as necessary Buabeng et al., (2020).

- **Clear Policies**

The policies that can be implemented are policies of fraud detection, prevention, and response within an organization. According to ACFE, 49% of fraud cases happened because of a lack or override of internal control, hence the significance of efficiency and implementation of these policies cannot be overemphasized. Such policies should, in the same way, be displayed or given to all employees and other stakeholders Eze, (2021).

- **Real-time transaction tracking**

Real-time transaction monitoring identifies and stops fraud as it happens meaning there is little to no loss for the business Sohel et al., (2024).

- **Effects of New Technology and Fraud Prevention**

There are several ways in which technology has the potential to support fraud prevention and identification efforts. This means that through the use of analytic tools and Machine learning, general patterns of data fraud can be recognized. Moreover, automation can bring about some pre-written standard work protocols for technical and business vocabularies, claiming that the use of computers to reduce degrees of imprecision sharpens the decision-making process and outweighs possible human influence leading to fraud Bello et al., (2024).

- **Standards in adopting Continuous Monitoring and Review**

Of course, fraud prevention is not an effort that occurs only once since fraud with globalization is ever-present. It is suggested that organizations must implement a regular audit of the whole concept of fraud prevention in an organization to ensure it is worthy of its name. These are as follows; engaging in daily checks and balances, regular policy and procedures, audits and risk review; and keeping abreast with various local and international fraud risks that may affect the organization Kerwin et al., (2021).

- **Inter-agency Cooperation and Information Exchange**

Among the guidelines, the approach to fraud prevention and detection includes the following: The cooperation between organizations, police, and surveillance agencies. Fraud Fights aims to provide organizations with the necessary knowledge of how to prevent fraud; the principle of fraud fight ensures that different organizations continually share this information and the best practices on fraud prevention thus making it difficult for fraudsters to pull off their tricks Kaur et al., (2023).

- **Combating Modernity in White-collar Cybercrime**

Criminals are using new platforms as the technological advancement of devices increases to perpetrate offenses. These risks must be known and addressed to understand and limit fraud and its detection in today's organizations. Such measures as ensuring illegitimate people have powerful protection, monitoring online transactions, and perhaps informing the organization's employees and customers about online fraud Ibrahim, (2022).

1.1.2 Historical Outlook of Fraud Prevention

Fraud prevention has been in existence even dating back to ancient societies with societies in existence coming up with different ways through which they could use in preventing fraud and for sieve it Torra-Prat, (2024). In the past, fraud was controlled by conventional processes like manual accounting and auditing, which indeed are highly exhaustive and very often inaccurate. New rules in the modern world are better due to advancements in technology by coming up with better techniques of checkpoints of fraud. With the help of computers and software, most of the organizational processes, which include accounting and auditing, conduct most of its transactions, and less chances of errors occurring Hamza et al., (2022).

In recent years new trends in fighting fraud have emerged changing traditional methods have shifted towards more progressive uses of artificial intelligence, machine learning, and data analytics. It covers how these technologies have helped organizations fight fraud by detecting it early, and how organizations can prevent fraud from happening in the first place Banerjee, (2024).

Technology Mitigating Fraud has embraced many names such as Identity fraud, phasing, Account takeover, and APP fraud to mention but a few. To this end, fraud has steadily developed beyond the first known case of insurance fraud found in Greece in 300 BC. However, the very first case of financial fraud was committed longer than that, around 500 years later in Rome Bojilov, (2023.).

In the present world, especially since the late 1980s, technology has developed the common frauds of handing out bad cheques, fake currency, duplicating credit cards, etc. The internet is a massive influence in the world and any person with a link to a computer now has it. Thieves are in a position to get hold of people's data and have been in a position to exploit countless amounts of innocent individuals Thangavel et al., (2023).

The number of fraud cases now seems to be on the rise at an exponential rate. According to a Federal Trade Commission report, there were more than 4.2 million fraud reports in 2021, 2.8 million fraud-related complaints, and 1.4 million idol theft complaints. While the USA population is nearly 5 times the population of the UK, in 2021 there were 445,357 fraud victims reported within the UK Ojolo, (2020).

The problems of fraud prevention have worried societies historically for millennia. From as far back as 2000 BCE the Sumerians and the ancients of Mesopotamia used clay tablets to record financial transactions and this early check and balance system helped to prevent mistakes and fraud. In ancient Greece and Rome there were legal acts that outlawed fraudulent actions, and put legal sanctions against embezzlement and corruption. In the course of the Middle Ages, manual techniques of accounting and auditing were also applied. These real processes were tedious and liable to incorporate inefficiencies, yet they ensured and checked on acts of fraud Kranacher et al., (2023). The technological revolution beginning with the creation of the printing press in the fifteenth century led to the reproduction, and consequently a more acceptable uniformity, of financial documents such as accountants' reports and auditors' reports. There are confirmed changes that the Industrial Revolution made in business activity: the use of new technologies and non-traditional ways of fraud detection and prevention. With the advent of the telegraph towards the end of the nineteenth century communication speed was improved and checks were placed on fraud cases including embezzlement Whalley et al., (2018).

In the twentieth century, an extensive multiplication of computers together with software was stressed as inventions that could facilitate the automation of business routines such as accounting and auditing. This lessened errors and improved efficiency but at the same time, it opened up new areas for endeavouring fraud. Over the past few years, there has been a change in focus on the adoption of artificial intelligence, machine learning, and data analysis for fighting fraud. These technologies have enabled organizations to learn patterns and oddities in data that may show fraudulent acts and prevent fraud occurrences in the future Sharma et al., (2024).

Advancements in Fraud Control: A Military Model

Many methods of fighting fraud have emerged gradually over the years. In the past solutions were mainly a reactive approach to prevent and mitigate fraud, organizations used rule-based approaches that involved fixed sets of criteria to look for. However, with the emergence of new technologies, fraud prevention has slowly turned into more preventive measures where organizations employ the use of analytics and machine learning to detect fraud Hilal et al., (2022).

The Employment Technology in the Prevention of Fraud

This paper looks at how technology has helped in shaping the strategies for combating fraud. Computers and software have played a significant role in simplifying most business necessities such as accounting and auditing where errors have been minimized, and efficiency enhanced. Artificial intelligence, machine learning, and data analysis have also enabled organizations to quantify data that might reveal dubious practices Karpoff, (2021).

Fraud Prevention: The Future

Hence, fraud prevention solutions in the future must be highly influenced by innovative features such as artificial intelligence, machine learning, data analytics, and others. These technologies will persist in being useful in detecting and specifically preventing fraudulence in organizations Rane et al., (2024).

Finally, in reaction to the surge in advanced fraud schemes, organizations will focus on preventing sophisticated fraud from occurring in the first place, by utilizing new and complex analytic and machine learning detection tools. There too will be increased cooperation between organizations, police, and other regulatory agencies to combat fraud. Since the earliest societies, the problem of fraud prevention has become an important question. Fraud prevention techniques over the years have been somewhat crude but developed over the years to where there is application of artificial intelligence, machine learning, and data analytics. It can also be predicted that the situation in the sphere of fraud prevention will be determined by shifts in progressing techniques on the molecular level, as well as the expanding role of preventive measures, cooperation, and exchange of information Rubio, (2023).

1.1.3 Prevention Measures of Fraud in the Departments

Fraud may manifest itself in any organization function and as a result, there is a need to check all functions of the organization. Here are some common fraud prevention strategies used in different departments:

1. Finance Department: As the finance department holds the finances of the organization, it is very important to put some controls to minimize fraud on the financial front. The finance department's anti-fraud controls implemented include the separation of tasks, treasury, and account balance checks, and computerized accounting systems Aye, (2023). The finance department's anti-fraud controls implemented include:
   - Separation of tasks: This involves decentralization of financial activities where the most complex and sensitive activities are divided in equal measures among many employees Altamimi et al., (2023).
   - Treasury controls: This comprises control of cash, control of accounts payable, and also control of accounts receivable Halder, (2022).
   - Account balance checks: Owning account balances frequently to conduct a quick check to identify any major or multiple anomalies Pagano, (2020).
   - Computerized accounting systems: Leasing computerized accounting systems to facilitate the financial transaction process and avoid problems associated with the human species Chen et al., (2020).

2. Human Resources Department: The management of the employee information is under the remit of the human resources department and therefore protection from identity theft and Human Resource Fraud has to be accomplished Yange, (2019). Fraud control measures utilized in the selection process carried out by Human Resource Management include background checks, audits, and the use of the HR management information system.

   Fraud control measures utilized in the selection process carried out by human resource management include:

   - Background checks: Admitting new persons who are hired into the organization to undertake background checks to confirm their identity and authenticity O'Neil et al., (2022).
   - Audits: From time to time run inspections on the HR unit to analyze discrepancies and/ or irregularities that may be present Halim et al., (2023).
   - Use of HR management information system: Installing an HR MIS that physically helps to manage and coordinate an organization's human capital through the elimination of possible human error Kaaria, (2022).

3. Operations Department: The relevance of such controls comes from the fact that the operations department is the department that handles all ongoing organizational processes and, therefore, is susceptible to operational fraud Biegelman et al., (2012). Some of the most common methods of carrying out fraud prevention measures in the operations department that were mentioned above include; The use of regular audits, the use of operational software to check on transactions, and the segregation of duties. Some of the most common methods of carrying out fraud prevention measures in the operations department that were mentioned above include Dimitrijevic et al., (2021):

   - Regular audits: Auditing regular operational processes to identify some distortions or variations.
   - Use of operational software: Operating applications to ease work, thus eliminating chances of entering the wrong figures in the account.
   - Segregation of duties: Splitting responsibilities within various job activities to minimize the level of authority those specific tasks have within one employee.

4. IT Department: The IT department is the unit in the organization that has the responsibility of managing its technology systems; it is thus strategic to institute measures that would reduce events of cyber criminality and other kinds of IT fraud. At the IT department, some

common precaution measures that can avoid fraud include firewalls, antivirus, and encryption of data. When institutions put measures against fraud in every department, they will minimize fraud incidences thus safeguarding their property Pomerleau et al., (2020).

- At the IT department, some common precaution measures that can avoid fraud include:
- Firewalls: Using firewalls that will block unauthorized access to the organization's network.
- Antivirus software: Using Antivirus Software for Malware detection & control.
- Encryption of data: How to protect the computer data to avoid getting by unauthorized personnel?

The necessity of the establishment of antifraud controls in every department

Whenever institutions place measures against fraud in all departments, they will prevent fraud incidences hence protecting their property. Implementing anti-fraud controls in every department is essential because Wells, (2017):

- It helps to prevent financial losses: It is worth noting that it is always easy for organizations to implement several anti-fraud controls that can help to reduce the number of monetary losses as a result of fraud activities.
- It helps to maintain reputation: Reducing fraud also contributes to the organization’s image since the prevention of fraud activities minimizes the violation of the organization's image.
- It helps to comply with regulatory requirements: This can go hand in hand with meeting customer needs since anti-fraud controls make organizations respond to meet requirements and additional rules, thus avoiding cases of penalties and fines.

Overall, strong guidelines against fraudulent processes within every department are mandatory to avoid fraudulent conduct and provide a favorable image of the organization’s business. That is why it is possible to speak about the necessity of carrying out departmental anti-fraud controls which differ from each other since every department has certain types of risks and susceptibilities. It demonstrates that anti-fraud controls can help organizations save money, protect their reputation, and meet industry regulations Hilal et al., (2022).

1.1.4 Impact of the Pandemic on the Prevention of Fraud

A significant change has been observed in the way the COVID-19 pandemic has influenced the way organizations work on their fraud risks. In the pre-pandemic era, most organizations implemented simple measures of analytics that before the pandemic included manual monitoring of transactions and physical auditing. However, the coronavirus outbreak led organizations to shift gears and experiment with new ways of working in particular, remote work and more digital transactions. As a result of the pandemic, organizations are forced to adapt quickly to new fraud prevention measures due to the ascending rates of cyber crimes and other types of fraud. This consisted of technology systems including artificial intelligence and machine learning as a way of tracking transactions and identifying unlawful ones. After the pandemic, the organizations have not left themselves with any chance and have made some further changes in their process of fraud prevention. For instance, it is quite evident that most firms have evolved high-intensity security systems to counter higher risks of cybercrimes Cherif et al., (2023).

The infection has also shown that organizations require more assertive and fast action in terms of fighting fraud cases. The remaining six are the actual activities of the fraud prevention framework, where the organization should constantly update itself on the threats and trends as well as update its employees and the effectiveness of the strategies implemented in the organization Saxena et al., (2020).

The COVID-19 pandemic situation has brought a lot of changes in how organizations are dealing with fraud. Before COVID-19, the vast majority of organizations employed traditional methods and basic statistical tools to track transactions and mitigate risks of fraud. That being said, the new culture of work-from-home and digital payments has made organizations implement new methods of preventing fraud quickly Wen, et al., (2023).

The pandemic has presented quite unknown and extraordinary societal issues such as the rise in the incidences of fraud. It was revealed that the scammers exploited the opportunities of the pandemic and acted especially in the spheres connected with big money, for instance, the oil and gas industry and those sectors that dealt with the pandemic response. There’s an increased realization of fraud risk over the years, and remedial measures need to be put in place to mitigate fraud. Through economic oppression, firms have had external and internal shifts which can make them vulnerable to exploitation. However, ongoing disruptions and economic uncertainty can put pressure on companies to defend their margins and also create opportunities for fraudsters to take advantage of unsteady systems and controls Levi et al., (2021).

Fraud may also facilitate money laundering, and terrorism financing and could devastatingly affect the reputations of the organization's shareholders besides customers. Managers needing to implement and monitor such a system should be proactive. Discover how the fraud triangle is shifting and how you can keep up Mohammadi, et al., (2020).

- **The Rise of Cybercrime**

COVID-19 recently has accelerated the rate of cyber criminality, the latter benefiting from the chaos and uncertainty generated by the virus. Organizations have had to adapt promptly to this kind of threat in recent years by integrating artificial intelligence and machine learning mechanisms in an attempt to monitor transactions and detect unlawful ones Choudhary et al., (2022).

- **The Development of Fraud Prevention**

The pandemic has consequently really impacted the trend in the development of anti-fraud models, indicating that organizations have shifted from traditional to modern methods. This has involved factors such as analytics coupled with mechanical as well as electric learning alongside artificial intelligence to deter fraud Zhu et al., (2024).

- **Speed and Agility as Considered Essential Factors**

The pandemic has also had a constructive effect on the mitigation of fraud, in which speed plays a crucial role. Such types of threats should be adaptable; thus the organizations need to be prepared to counter them as and when they emerge. This in turn demands high levels of flexibility and readiness to court trial and error Zhang et al., (2022).

- **Employee education and awareness play this role:**

Other measures focus on more employee education and improved awareness of fraud risks are also important. Companies have the responsibility to inform their staff of potential losses due to fraud and the general possibilities of fraud detection. This ranges from educating its employees when, where, and how to recognize phishing scams, different methods of reporting them, or using IT to mitigate fraud Taherdoost, (2021).

- **The Requirement of Interminably Checking**

The pandemic has also pointed to the fact that there is a need for constant review of every fraud prevention measure put in place. It must manage to adapt to the strategies it uses frequently and where necessary update them so that it can counter emerging risks Alawida et al., (2022).

- **The Implication of Partnership**

Last but not least, the pandemic has proved that combating fraud is impossible without cooperation. There is a need for organizations to share what they know, as well as learn from each other to counter new trends Levi et al., (2022).

- **Why Fraud Prevention Is the Future**

That is why threat actors' approaches to fraud, which have evolved significantly over the pandemic, will determine the future of fraud prevention Ma et al., (2021). Subsequent threat types and technological advances will likely force organizations to remain more flexible and obtain higher velocity and depth of employee education and awareness. In this way, they will be able to adapt to changing threats in the market to guard both themselves and their customers against fraud.

The pandemic has affected the fraud prevention landscape and the way organizations carry out this process a great deal. The circumstance organizations have adapted well to remote working and new variants of digital transactions have also made fraudsters come up with new modalities that require organizations to adopt fast new methods such as big data and analytics, machine learning, and artificial intelligence to counter-check. The pandemic has also brought to the fore speed and therefore agility, employee education, awareness, monitoring, and collaboration to deter fraud. This is because, with the ongoing effects of the pandemic, it is important for organizations not to relapse into complacency and do nothing about fraud Koerniawati, (2021).

1.1.5 How effective the Fraud Prevention Mechanisms are.

The functioning of mechanisms for fraud prevention is one of the important factors in the evaluation of an organization's risk management activity. As shown earlier, fraud prevention mechanisms are useful tools to fight and identify fraud situations, while facing some significant problems among organizations implementing them Bartsiotasm et al., (2016). The first challenge when implementing fraud prevention measures is that threats and techniques are ever-changing. Frauds are not relenting in their quest to explore the various forms of loose screws and cracks in an organization and how to deceive the check and balances. Another difficulty is the fact that fraud prevention should be proportional. There is always a tension between the desire of firms to deter and identify fraud and the desire to limit the costs of fraud prevention and detection on otherwise legitimate processes and activities. Organizations can not underestimate the human factor within the fraud prevention and detection process. Knowing employee awareness is crucial in any anti-fraud mechanism given the employee represents the first layer of fraud defense. The effective functioning of the fraud prevention mechanisms is not an impossible task and there are several examples of such mechanisms in practice. For instance, the application of big data analytics and artificial intelligence delivers outstanding results in fighting fraud Wells et al., (2017).

Another aspect that should be taken into consideration in assessing an organization’s risk management activity is the effectiveness with which different mechanisms for fraud prevention are operating. It has been evidenced above, that anti-fraud tools are useful instruments to struggle and detect fraud occurrences, but they encounter essential issues among the organizations applying them Erbuğa et al., (2022).

Assessing the Impact of Fraud Control Measures

In addition, it should be noted that it is also necessary to control the efficiency of the fraud-preventing tools and mechanisms which seem to have been implemented adequately. This includes evaluating how effective the mechanisms are in mitigating; Identifying; and Undertaking action against fraudulent practices. An efficient fraud prevention and detection model has to help identify and stop fraud before it takes place, detect fraud and act at the same time, and reduce fraud loss as much as possible Peiris et al., (2021).

Influences on the Implementation of the Fraud Control Measures

In this sense, we can identify several factors that may influence the efficiency of fraud prevention measures. These include:

- The complexity of the mechanisms: Intricate Sensory-motor patterns are not easy to deploy, and the intricacy lessens their performance Taufik, (2019).

- The level of employee awareness and training: Those who are informed of the mechanisms and their proper usage will be more capable of preventing or at least detecting fraudulent operations Shonhadji et al., (2021).
- The level of management support: Top management support remains an essential factor in the effectiveness of the anti-fraud controls. Where there is a lack of support from managers and leaders of the organizations, the mechanisms may not be put into practice or even if they are put into practice, they may not be well observed Maulidi et al., (2021).
- The level of technology used: There is an opportunity to develop fraud prevention tools with the help of modern technologies like artificial intelligence or machine learning Shoetan et al., (2024).

A Review of Key Strategies on Fraud Control and Prevention

Below are some practices that organizations should follow while implementing the best practices for fraud prevention Maulidi, et al., (2021). These include:

- Establish a culture of risk self-assessment to review their institution's vulnerability. Following sound anti-fraud control with policies and procedures in addition to controls
- Employee training and awareness programs are an important way of letting the employees know of their existence, their utilization mechanisms, etc
- Looking at how these mechanisms are effective or not continuously.
- Introducing novel applied technologies into the mechanisms, in particular, artificial intelligence and machine learning.

It can be sensed that antifraud measures play a significant role in the achievements of an organization. This sort of assessment helps organizations to check whether the mechanisms alleviate the risks of fraud, and if the deception is identified, whether the measures significantly deter it. Some of the knowledgeable factors include the level of complexity, awareness level of employees, levels of management support, and technologies employed within organizations. If the above-described best practices are followed, risk assessments are performed periodically, an anti-fraud program is comprised, the organization’s employees undergo training sessions and awareness programs, the effectiveness of the mechanisms is monitored and evaluated, and technologies are applied to improve the effectiveness of the mechanisms, organizations can implement efficient anti-fraud measures Bartsiotas et al., (2016).

1.1.6 Sectoral and Organisational Size Difference

ACAIs are aware that fraud prevention strategies may differ widely depending on the sector and the size of the organization. For instance, some organizations operating in the financial industry may be more likely to have well-developed fraud prevention policies than organizations in other industries Bodker et al., (2023). Farmer & Schaeffer further observed that small nonprofits have different characteristics; they are likely to possess limited resources and, therefore, have to depend on intensive and conventional procedures in the detection of fraud. Fraud risk for organizations in various sectors may not be the same, there may be variations in fraud risk type. For instance, organizations in the retail industry may be at a higher risk of credit card fraud as compared to organizations in the healthcare industry may be at a higher risk of identity theft. It is also important to understand that large organizations will have more advanced and modern methods of fraud control systems implemented in contrast to small organizations which will need to carry out the methods manually or more traditionally Fish et al., (2020).

Still, it is important to emphasize that fraud risks are present in every sector and at every organizational size; therefore, all organizations should come up with effective strategies for fraud prevention and act and be ready to adjust the strategies to the current conditions. This involves ensuring that the organization has adequate knowledge of the current threats and trends and the extent to which employees are protected, ensuring adequate provision of employee education, and familiarizing the organization with the efficiency of the different fraud prevention measures Khando et al., (2020).

Of course, the sector and size of an organization unquestionably determine the general nature of fraud threats and the most effective means to combat them, but it is necessary to admit that fraud threats are relevant to all organizations, no matter how successful and reliable they are Rybalchenko et al., (2022). Fraud prevention is crucial in any organization no matter the nature or size of the business, this includes giant international business organizations or small-scale family businesses.

For example, the financial services industry has been and continues to be vulnerable to attacks primarily because of the nature of the information worked with as well as the value of the assets processed. This means that fraud costs banks, insurance companies, and investment firms have forced organizations to put in place complex fraud detection mechanisms, use analytical tools, and conduct regular checks on datasets. In addition, they need to make the employees aware of the contemporary fraud risks and ensure that someone stops fraud as soon as possible Uddin, et al., (2020).

That is why the challenges related to the healthcare sector are different; they include medical identity theft, healthcare fraud and prescription drug abuse. Regarding patient data, healthcare institutions need to ensure its security, as well as confirm the prescription's genuineness, and control access to high-risk systems. Further, they should coordinate with the police to fight against fake healthcare practices and switch details about the rising hazards Goel, (2020).

The retail industry, contrary to other industries, is not frequently linked to fraud cases, however, it is a potential target for point-of-sale frauds, merchandise frauds, IT frauds, or cyber frauds. Retailers need to develop highly secure information technology protection, educate people working in stores about possible scams, and provide proper inventory controls. Further, they should implement omnichannel fraud prevention measures since their stores and online platforms will be affected by Almalki, (2022).

Typically, small and medium businesses (SMEs) may have serious difficulties with initiating systematic anti-fraud measures since they do not possess resources and qualified personnel Bishop, (2022). However, they are capable of finding ways to reduce their exposure to fraud risks. These include:

- Employee training: Increase the awareness level of the employees about fraud risk, fraud indicators, and reporting mechanisms.
- Strong internal controls: Setting of proper measures for the security and protection of the assets fragile to malicious interferences.
- Regular reviews and audits: Voluntary checking of the financial documents as well as business activities to assess the likely risks.
- Vendor due diligence: Checking on all suppliers and vendors to reduce cases of fraud being conducted.
- Cybersecurity measures: Preventing unauthorized access and infiltration of networks along with spam and identity theft, viruses, and malware.

Indeed, technology brings lots of opportunities with it, but the occasion also brings a nasty side with it, particularly fraudsters. This is because artificial intelligence, smart machines such as machine learning, and big data analytics are being employed in cases of fraud detection.

Businesses cannot afford to sit idle while these advancements are made and also cannot afford not to invest in effective countermeasures to stop the hackers Banerjee, (2024).

1.2 Research Problem

Fraud prevention has emerged as a major issue of concern for organizations in the recent past due to the large monetary and image losses organizations tend to suffer from Occupational Fraud. When organizations learn how to respond to ever-changing conditions of the business environment, particularly about the recent pandemic crisis of COVID-19, the role of organizing adequate anti-fraud measures becomes even more important. The purpose of this research is to explore the contemporary problem related to fraud prevention in organisations while focusing on the effects of anti-fraud measures in occupational fraud. The aim of this study is therefore to add value to solving the challenges encountered in the current research area through examining the major approaches utilised by organisations and the changes made after the pandemic.

The first research problem seeks to establish the major anti-fraud controls that are currently in use by organisations, bearing in mind that these controls differ within various organizational units like HR, accounting and finance, operations and IT and others. Throughout the pandemic, companies have changed their fraud prevention strategies concerning new risks like distant work, fragile supply chains, and instability. Common practices used by organizations include internal controls, audits, background checks and awareness training, and information technology innovations such as data mining and fraud fighting software. It also plans departments to work on different aspects of fraud prevention depending on their duties and responsibilities. Wells, (2017.) Using models for the Accounting and Finance departments, the focus can be on internal control, while models that can be applied in the HR department, the highlight will be given to screening and training of employees.

The second research problem looks at whether the organizations have changed any elements of their existing fraud prevention programs due to pandemic and if there are improvements made to the programs after COVID-19 to prevent occupational fraud. There are new fraud risks and new challenges which appeared during the pandemic, like cybersecurity, fake loans, and social engineering scams. To tackle these matters, the adaptations that have been adopted include remote fraud monitoring tools, more training on pandemic related scams among the employees and enhanced cybersecurity measures. Morales et al, (2014) These changes reflect the emerging fraud environment and seeks to safeguard organizations and their operations.

The third research question aims at establishing to what extent post-pandemic changes to the fraud prevention had been efficient in combating occupational fraud across different departments and how efficient factor differs across departments. Evaluating the success of such adaptations is something important in ascertaining the success of organizations in the fight against fraud. This research, through assessing the effects of such changes, will establish improved approaches for fraud prevention and reveal existing flaws in the existing anti-fraud strategies of various departments.

Lastly, the fourth research problem is concerned with the similarity or otherwise in the approaches to fraud prevention in organizations of different size and in different sectors as well as the formulation of department specific approaches to build the organizational resilience toward occupational fraud. This will mean a comparison of the measures taken by these organizations depending on their type, for example those of SME’s and large companies. These differences can then be used to develop specific strategies that fit each department’s fraud risks, thus improving the strength of the overall framework in fighting fraud.

Consequently, this research is a response to the present anomalies of managing fraud prevention in organizations through the analysis of the effects of anti-fraud controls on occupational fraud. The extent to which key fraud prevention mechanisms have been impacted post-pandemic, the effectiveness of these adaptations within each department, and the differences in approaches between organisations will support the current area of research to overcome the mentioned challenges within this study. Promisingly, the findings received from this investigation will assist organizations in enhancing fraud prevention and response as more specific, systematic and stronger occupational fraud barriers.

1.3 Purpose of the study

This paper seeks to identify and critically assess adaptation made by organizations to current methods used in preventing occupational fraud and factors of adaptation, including post-pandemic changes. This paper aims to have an understanding of available solutions and strategies put in place to reduce fraud within organizations, in the departments being exposed to risk, and during the current COVID-19 pandemic Stapleton, (2022).

To achieve this aim, the study has the following specific objectives:

- To explore the currently utilised fraud prevention mechanisms across various departments in organisations.
- To examine and document the specific modifications made to fraud prevention mechanisms in response to the global pandemic across various departments
- To evaluate the effectiveness of fraud prevention mechanisms within various departments, focusing on the impact of post-pandemic modifications on the prevention of occupational fraud
- To identify and compare the commonalities and differences in fraud prevention approaches employed by organisations across different sectors and sizes

Objective 1: To explore the currently utilised fraud prevention mechanisms across various departments in organisations

This objective can be to analyze the current antifraud controls about employees including human resources, accounting, finance, operational, IT, and all other departments. This research will therefore set out to determine the kind of fraud prevention strategies currently in practice and evaluate their efficiency in combating occupational fraud Akinbowale et al., (2023).

Objective 2: To examine and document the specific modifications made to fraud prevention mechanisms in response to the global pandemic across various departments

The specific focus of this objective is to describe changes that occurred in implementing fraud prevention measures after the COVID-19 pandemic outbreak. The formalized research question is, therefore, as follows: To what extent have fraud prevention mechanisms been modified in response to COVID-19? Ma et al., (2021)

Objective 3: To evaluate the effectiveness of fraud prevention mechanisms within various departments, focusing on the impact of post-pandemic modifications on the prevention of occupational fraud

Due to this objective, any changes made after the pandemic or otherwise to protect from fraud will be assessed and their efficiency in preventing occupational fraud within the departments will be judged. The research will evaluate the efficacy of fraud containment measures within the company and in particular examine the measures in the HR, Accounting, Finance, Operation, IT departments, and other related organs to realize the measures most efficient in discouraging occupational fraud Levi et al., (2021).

Objective 4: To identify and compare the commonalities and differences in fraud prevention approaches employed by organisations across different sectors and sizes

To this end, this objective seeks to explore the similarities and variations in fraud-fighting measures used by organizations irrespective of the industries and within various categories of organizations. The research will examine the varieties of measures the organizations in various categories of industries of the micro, small-medium, and large companies used to curb occupational fraud and to what extent these measures provided the needed deterrence towards the fraudsters HAKAMI et al., (2019).

1.4 Research Questions:

- What are the key fraud prevention mechanisms currently employed by organizations, and how do these mechanisms vary across different departments, including HR, Accounting, Finance, Operations, IT, and other relevant departments?
- How have organizations modified their fraud prevention mechanisms in response to the global pandemic, and what specific adaptations have been made post-pandemic to enhance resilience against occupational fraud?
- To what extent have the modifications made to fraud prevention mechanisms post-pandemic been effective in preventing occupational fraud within various departments, and how does this effectiveness differ across departments?
- What commonalities and differences exist in the approaches to fraud prevention among organizations of different sizes and in different sectors, and how can these variations inform the development of targeted, department-specific strategies to enhance overall organizational resilience against occupational fraud?

1.5 Significance of the Study

Fraud is a constant menace to all forms of businesses and organizations regardless of their size and location. With the emergence of the recent coronavirus pandemic, the nature of work has changed, and therefore organizations require efficient strategies for the prevention of fraud. There are similarities as well as differences between size and structure of different sectors of industries and organizations. The identity of the strengths and limitations of today’s existing fraud prevention mechanism requires a comprehension of present day’s prominently used fraud prevention mechanisms. Nakitende et al, (2024) Thus, the relevance of this study will be in offering a ‘snap-shot’ perspective on the existing status of Anti-Fraud measures implemented within a multiple-Department environment. Thus, the study focuses on evaluating the current state of measures within HR, Accounting, Finance, Operations, IT and other departments; recognizing their best practices, weaknesses and opportunities for development. These research results will be useful to the current stakeholders and decision makers to understand the adequacy of current functional fraud prevention measures and extend these measures to reduce fraud.

The effect of the current worldwide outbreak on the frameworks against fraud prevention remains an essential theme for investigation. The new conditions posed by the trend to remote work, lockdowns, and changes in the overall economic environment left businesses and organizations with no choice but to reimagine their approaches to fraud prevention. This research aims at investigating the changes that organisations have made on their fraud prevention systems after the pandemic and assessing the efficiency of these changes as well as identifying how the efficiencies of these changes can be harnessed for better organisational fraud prevention. The analysis of the post-pandemic environment will help to develop an understanding of how to manufacture protective frameworks in a way that guarantees that they and the organizations that employ them are prepared for subsequent catastrophes. Galbraith et al, (2024) Another important aspect of this work is an evaluation of the efficiency of fraud prevention measures implemented at the various organizational departments and identification of the changes made after the pandemic process. In so doing, the research seeks to establish effectiveness of these measures in the fight against occupational fraud and thus identify best practices together with gaps that could be closed. This evaluation would help towards a better understanding of the approaches which can be best used in preventing fraud and also help organizations in the implementation of better and more all-round methods of protecting their property and data.

This research aims to compare and contrast the anti-fraud strategies and measures used by organizations regardless of industry type and business scale. Cross-sectional research on the fraud prevention efforts of firms in different sectors and employing people from all walks of life will highlight the antecedents explaining the implementation and performance of such procedures. Based on the findings of this analysis, organisations will be able to compare notes and make better decisions about their fraud fighting measures in the hope to build a stronger environment for the safety and stability of businesses. Therefore, the importance and focus of this research stems from the presentation of an exhaustive view of modern anti-fraud tools, changes in response to the pandemic, and outcomes of the modifications. This research will add value to the field of fraud prevention by comparing organizations' experiences across sectors and organizational structures, helping the development of better, more flexible, and efficient fraud prevention practices and initiatives.

CHAPTER II: LITERATURE REVIEW

The second chapter of the thesis provides a complete review of the existing literature that is related to the area of research. The section reviews books, articles, academic journals, etc to provide insights from secondary literature that is publicly accessible.

2.1 Theoretical Framework:

The understanding of occupational fraud has been significantly shaped by two key theories: the Fraud Triangle and the Fraud Diamond. These theories assist in the evaluation of the situations that enable fraud and the attributes that make it possible for an individual to engage in fraud.

2.1.1 Fraud Triangle Theory:

The "fraud triangle" is a notion that fraud prevention professionals and researchers commonly use to predict the circumstances that contribute to a high probability of fraud. Steve Albrecht used criminological studies by Edwin Sutherland and Donald R. Cressey to simulate the circumstances that increase the likelihood of fraud. "People have an incentive to engage in fraud when the following factors come together: (1) some kind of perceived pressure, (2) some perceived opportunity, and (3) some way to rationalise the fraud as being in line with one's values," according to Albrecht, who developed the fraud triangle Pararas, (2023). The Fraud Triangle is an FRI and occupational fraud theory originated by criminologist Donald Cressey in 1953. It identifies three primary elements that must be present for fraud to occur: The three abstractions include pressure, opportunity, and rationalization acknowledged by Cressey in his study of embezzlement. This theory posits that in order to meet various important financial and personal obligations people may be forced to engage in fraud. Exploration of an opportunity, for instance, weak internal controls or little supervision, makes the individual carry out the fraud and justify the action.

It has been vital in regards to the development of anti-fraud measures especially in considering the factor of perceivable opportunity. Albrecht et al, (2012) pointed out that opportunities for fraud are thereby reduced by the effective internal controls. But the two other elements, pressure and rationalisation, are challenging to combat directly as they have to do with individual incentive. Wells (2017) notes that failures in these areas are the reasons why organizations should encourage ethical business values and extend help to stressed or financially troubled employees.

2.1.2 Fraud Diamond Theory:

Considered to be a more comprehensive version of the Fraud Triangle Theory, "The Fraud Diamond Theory" was initially introduced by Wolfe and Hermanson in the CPA Journal in December 2004. To the three original elements that make up fraud in the Fraud Triangle Theory, an additional component called "Capability" has been introduced in this theory. Fraud is unlikely to occur unless the capability, or fourth ingredient, is also present. Stated otherwise, the individual who could perpetrate fraud needs to possess the necessary abilities and capabilities. The ability to identify a specific fraud opportunity and make it a reality is known as capacity Elbagoury, (2023).

Wolfe and Hermanson (2004) expanded on the Fraud Triangle by introducing the Fraud Diamond Theory, which adds a fourth element: capability. According to the Fraud Diamond, even if there is pressure, opportunity and rationalization for fraud in an organization, this cannot happen without an enabling capability. This capability means that the individuals involved in the organization have the right skills, the authority and self-confidence to capitalize on loopholes without getting trapped.

The Fraud Diamond theory has focused on internal controls as a way of minimizing the chances of fraud by reducing the options open to a fraudster with the skill set to defraud an organization Dorminey et al., (2012). For instance, firms should adopt better controls on access to resources and isolation of duties to reduce the risk of the misuse of power to defraud.

In regard to the Fraud Triangle and Fraud Diamond theories, both of these concepts can be commendable in achieving the task of defining the circumstances when occupational fraud can take place. These theories will be discussed in more detail in the successive sections of this literature review concerning the practical application of fraud protection measures, especially regarding the pre- and post-pandemic fraud risks.

2.2 Fraud Protection Mechanism Before Pandemic

Businesses are implementing several strategies to lower the incidence of fraud. They employ both internal norms and guidelines—also known as reactive mechanisms—as procedural remedies in this regard. They also employ proactive mechanisms by creating separate departments within organisational structures, whose duties include investigating fraud phenomena and ensuring that reactionary systems are operating as intended. As previously said, whether the corporation gets additional backing from the laws of national, EU, or international law depends on the organisation's field of activity. Nevertheless, the effective protection of the organisation against fraud is not ensured by the mechanism's application in any form Skoczylas-Tworek, (2019). Kamaliah et al. (2018) investigate the degree to which public systems' monitoring procedures are preventing fraud instances. According to the findings, asset misappropriation is often the most common fraudulent instance in government organisations. Regression analysis revealed that internal processes or policies significantly decreased the number of fraud events. Furthermore, a strong correlation has been demonstrated between the prevalence of fraud in government institutions and both good governance and fraud prevention initiatives. The study gives public employees valuable knowledge about the efficacy and utility of internal control protocols, good governance practices, and fraud prevention initiatives in the public sector.

Denman (2019) provided that fraud is as common as it has ever been, if not more so. Boards and upper management must therefore devise strategies to stop and identify fraud. An anti-fraud policy must be adopted and adhered to without fail. Next, a fraud risk assessment must be conducted to identify the business's most vulnerable areas. After that, the top management of the company needs to implement safeguards that will stop and identify employee fraud and keep an eye on them to make sure they stay in place. Even while not every fraud will be prevented by these safeguards, the organisation can at least work to lessen its impacts. Mouamer et al. (2020) determine how using career fraud detection and prevention technologies can help fight and prevent fraud while lowering its risks by conducting a field investigation on the Palestinian Ministry of Health in the Gaza Strip. The study concludes that respondents gave the MOH's use of tools to detect and prevent job fraud a favourable evaluation, and they showed a strong interest in these tools when it came time to put them into practice. The study suggested that in order to ensure the avoidance of conflicts of interest, particularly for the group of doctors, the Palestinian National Authority should draft and endorse laws governing the healthcare industry. This will prevent doctors employed by the government from having two jobs. The research also suggested that MOH embrace healthcare governance concepts and start putting them into practice right away.

Shepherd and Button (2019) look at organisational barriers to dealing with occupational fraud. A variety of avoidant justifications developed by organisational victims' advocates to support ignoring occupational fraud. The paper contends these justifications form a theory of differential rationalisation since they are quite comparable to the justifications given by offenders. Managers avoid taking proactive measures to prevent fraud in the workplace and ignore incidents that are reported unless they feel that doing nothing will have a greater negative impact than dealing with the issue. Higher than "normal" fraud losses, the glaring nature of the frauds, and the proactive involvement of an outside organisation, such as senior management or a strong counter-fraud department, are some of these scenarios. Suh et al. (2019) aim to quantify the correlations between various fraud risk characteristics and the perceived "opportunity reduction" in terms of the "likelihood of fraud occurrence" in financial institutions. The likelihood of reporting a past instance of fraud at work is negatively correlated with the qualitative component of opportunity reduction by means of the perceived efficacy of anti-fraud oversight, but not with the quantitative component of opportunity reduction (the quantity of anti-fraud controls). The research's primary conclusion is this: operationalising mechanisms for control effectively prevents fraud more than having anti-fraud controls in place alone. This supports the idea that content matters more than form and confirms that outdated controls are useless.

Nawawi and Salin (2018) examine the internal control gaps in the spending claim process and find out what the employees think about occupational fraud. The analysis discovered that the business's internal control is insufficient and feeble. The majority of respondents concurred that in order to stop occupational fraud, internal surveillance needs to be strengthened and updated. Every department, but the finance division, in particular, has a crucial responsibility to oversee the effectiveness of internal control. The primary issue is that internal controls ought to be able to both streamline the current procedure and stop fraud from happening. According to those surveyed, there is a correlation between an organisation's ability to prevent occupational fraud and its level of internal control. When workers have a high level of awareness about occupational fraud and are eager to report instances of fraud to management and provide assistance when needed, this is a positive sign. If a whistleblower receives just compensation, the employees of the company are likewise incentivised to support the organisation. Singh (2020) assessed the contribution of fraud awareness to the development of a fraud prevention culture in an administrative unit at a university in South Africa in order to avoid occupational fraud. The investigation verified that there could be a danger of occupational fraud in the division. The most prevalent is staff bribery. Results further supported the importance of raising knowledge of fraud in order to avoid occupational fraud and foster a culture that opposes it. Furthermore, this study offers evidence in favour of applying both theories to stop occupational fraud and foster a culture that opposes fraud. The study's conclusions included suggestions for improving the efficiency of the department through actions to raise staff involvement in preventing fraud, raise fraud awareness, and foster an anti-fraud culture.

Davis (2019) investigated internal control techniques Six small-business proprietors in the southeast region of Pennsylvania were employed in the past to stop and identify workplace fraud. The study's conclusions included suggestions for steps owners of small enterprises might take to stop and identify occupational fraud. Proprietors can use employee identification papers to monitor employee behaviour, separation of roles, interaction with employees, and surveillance as strategies to safeguard their companies against fraud at work. The research's implications for beneficial social change involve the possibility for social entrepreneurship, whereby owners of small enterprises give community members—including high school students who aspire to operate small retail businesses—work opportunities. Ortiz (2018) examines the tactics employed by certain proprietors of small eateries to lower the incidence of occupational fraud. Relatives, internal audits, and surveillance systems are necessary components of a successful owner's monitoring program. The application of analytical processes and a sufficient division of labour for cash, inventory, and sales transactions were also mentioned by those surveyed. Owners may take into account internal memoranda, procedural manuals, and written guidelines for their communication approach. A persistent business risk that has an impact on an organisation's profitability is employee fraud. Company executives can successfully lower this risk to the company while fostering the development and profitability of the company. Business executives and professionals may enhance earnings, lessen occupational fraud, and foster community trust by implementing the study's conclusions, all of which will benefit society as a whole.

This paper aims at analysing the various fraud protection mechanisms that were in practice before the COVID-19 pandemic in order to reduce the risk of occupational fraud in organizations. Such initiatives entailed internal controls, auditing, fraud risk management policies, data monitoring, analyses, and control consciousness campaigns. The nature of these mechanisms was not in doubt; however, there were still problems – such as the ability to respond to technological advances and ever more complex forms of fraud.

2.2.1 Internal Controls as well as Auditing

Apparently, internal controls have always been viewed as an essential fundamental step that can help prevent fraud. These controls are so set to provide understanding, responsibility, and adherence to the organizational policies. Some of them are: Separation of responsibilities, approvals and documentation of various financial activities COSO, (2013).

In support of its assertion, Albrecht et al. (2012) posit that adequate internal controls are one of the best ways of combating occupation fraud. Internal and external audit complements these controls by independently reviewing the financial data and business processes periodically and identifying major or minor susceptibility from fraud. Nevertheless, the literature reveals some limitations of the traditional internal control systems. As Bierstaker et al. (2006) note, the vast majority of organizations have in place adequate internal control systems, however these systems are described as taking a relatively ‘reactive’ approach, unadjusted to reflect changing opportunities on a timely basis to the fraudster.

2.2.2 Fraud Risk management policies 100

However, it is evidenced that organizations have developed broad fraud risk management policies to reduce risks of occupational fraud. Some of these policies include; holding risk analysis exercises, creating methods of verifying fraud, and even creating plans on how to undertake an instance of fraud Kramer, (2015).

According to the Association of Certified Fraud Examiners (ACFE) (2019), enterprises with existing fraud risk management programs have a high likelihood of identifying fraud. These programs normally include the whistleblower’s hotline and the anonymous reporting systems which enables employees to report cases of suspicious activities and none will be subject to bargaining upgrades or termination. For example, Pope and Lee (2019) argued that these programmes remain crucial in promoting corporate culture of disclosure and resolution.

2.2.3 Data Monitoring and Analytics

While business processes moved online, organisations started utilising data monitoring and analysing as critical methods for fraud management. This makes it possible for organisations to monitor and analyse their financial records, conform employee activities and recognize any outliers in real time Baldwin & DiGabriele, (2018). The other major advantage of utilizing complex data analysis techniques, such as data mining, which incorporate AI and machine learning capabilities, is the ability to recognise patterns or deviations that may well indicate fraudulent transactions Holtfreter, (2015).

Before the pandemic, data monitoring systems were used in industries they considered having numerous transactions, which include banking industries and the retail business. As highlighted by Huber and Scheytt (2019) these systems provide indicators that evidenced the effectiveness in the industries to curb fraud, allowing intervention at the right time.

2.2.4 Stipulation of Employee Recognition of the Compliance Programs

Other procedural measures also aimed at combating fraud pre-pandemic included employee training, and awareness. Most companies embarked on prompting their workforce on fraud risks, how to avoid them and the need to follow regulatory measures Singleton & Singleton, (2011). Wells (2017) noted that employees spot fraud earliest within organizations and therefore, qualified staff are a good antidote to fraud.

According to Zhang et al. (2019), the organisation implemented a highly inclusive preventive measure by investing in integrated employee training, this ensured that when fraudsters exhibited tainted behaviors within the organisations employees reported them promptly, thus reducing organisational fraud incidences. Retraining is therefore a crucial aspect which should form part of an organization’s recognition program to fight fraud.

2.3 Pandemic and Post-Pandemic Fraud Risks

The COVID-19 pandemic, which indirectly forced nations to come together as a result of a serious threat to medical treatment, and new, a bit secondary kind of white-collar criminal behaviour that cross state lines are both either directly or indirectly triggered by the global epidemic. These challenges have been caused to the contemporary, interconnected world in 2020 and 2021. This necessitates increased collaboration between law enforcement authorities in the fight against emerging types of white-collar crime (WCC) on a global and national scale Kamensky, (2021). Levi and Smith (2022) highlight a few new crime categories and tactics that have emerged in the current pandemic that have not been seen in earlier pandemics. These modifications might be the consequence of COVID-19-related public health responses, the state of technology at the time, and the actions of law enforcement and regulatory authorities. It demonstrates that while many frauds would still happen, certain types of scams—mostly internet ones—occur during pandemics. Additionally, a great deal more opportunity was generated by COVID-19 than in prior eras due to extensive government aid programs for both individuals and corporations. The researchers emphasise that more early monitoring and control of fraud and related corruption in procurement must be a part of strategies for global epidemics in the future, and they add that this will require more political will and structure. Levi and Smith (2021) aims to highlight the similarities between frauds linked to pandemics and to pinpoint any hazards specific to outbreaks and financial crises, starting with the 1918 Spanish flu pandemic, which is thought to be the most similar to COVID-19 in the contemporary age. According to the report, the COVID-19 pandemic of 2020 was distinct in that governmental and corporate databases could be tracked and analysed to see how certain forms of economic crime evolved during the pandemic thanks to developments in ICT. Additionally, since the start of the COVID-19 epidemic, there has been a greater level of systemic public awareness regarding fraud and internet fraud that harm people. While baseline data on the effects of fraud is more accurate than for any prior worldwide event, tracking of fraud trends is not as developed as tracking of the rates of infection and deaths brought on by the pandemic.

Ma and McKinnon (2021) employ conventional criminological and psychological methods to investigate cyber security risks and cyber fraud victimisation during COVID-19. The modern information economy has been shaped by COVID-19, and it will keep shaping the connections between various actors in cyberspace. The digital economy will adjust in tandem with our efforts to mitigate the hazards of COVID-19 by implementing social distancing policies and shifting our daily activities online. This will involve changes to informative production and informational networks on an international scale. As a result, the risks associated with cyber fraud are increased in this pandemic environment. The internet's intrinsic privacy and cyber security dangers become societal and occasionally legal concerns, even while it offers the links and flexibility that are desperately needed in this unparalleled global crisis. The consequences of cybercrime and abnormal online social behaviour put laws and regulations pertaining to international authority at jeopardy. Technology has led to the emergence of cyber fraud, which has progressively influenced the global sociotechnical system within the framework of political economy. Emerging dangers of cyber fraud demand immediate action from a range of public and commercial sector stakeholders.

Monteith et al. (2021) look at how technology is being used differently, how the epidemic is affecting society, how cybercrime is developing, how vulnerable each person is to it, and how people with mental illnesses are particularly affected. Although technology offers strong instruments, these instruments must be utilised with the proper safety precautions. Because "individual behaviours, personality characteristics, online activities, and attitudes towards technology impact susceptibility, human factors" play a vital role in cybersecurity. Patients with mental illnesses may be more susceptible to cybercrime, but they may also be unaware of the risks and potentially dangerous online behaviours as well as risk-reduction strategies. Psychiatrists must be aware of the possible effects of cyberattacks on mental health as well as the elevated risk that patients face as a result of the epidemic, particularly with regard to online mental health services. Śmiałek-Liszczyńska and Wojtkowiak (2023) discussed the issue of identifying occupational fraud risks in remote employment and how they affect the control measures that managers put in place during the epidemic. The interviewees failed to mention any common frauds that deplete the company's assets or other intentional actions against the employer that were especially related to remote work (and had never been seen previously). Yet, the investigation turned up evidence of fraudulent conduct and control pertaining to working hours (staff availability) and efficacy (widely defined as staff productivity and effectiveness).

Darsono et al. (2024) look into fraud including asset misuse during the COVID-19 pandemic. According to the study's findings, employee asset misappropriation is influenced by pressure. Employee pressure intensified during the COVID-19 epidemic, increasing the risk of asset embezzlement. The fraud diamond idea states that there is a positive correlation between opportunities and staff asset theft. Increasing misappropriation of assets is a result of internal control shortcomings, which are especially evident in times of crisis such as the COVID-19 epidemic. These weaknesses include confusing duties, inadequate monitoring, unauthorised transactions, and inadequately documented processes. Additionally, there is a strong correlation between rationalisation and asset misappropriation, suggesting that workers who rationalise fraudulent acts are more likely to misuse assets. Additionally, capability exhibits a positive correlation with asset misappropriation, indicating that high-ranking personnel who are able to identify and take advantage of control system flaws are more likely to perpetrate fraud. McCormack (2022) examines the methods employed by financial firm managers in Kingston, Jamaica, to stop occupational fraud. To stop occupational fraud in companies, no one antifraud tactic is adequate. In addition to creating a compliance culture, leaders need to design and execute fraud detection and prevention methods. According to the results, supervisors of financial sector companies who wish to eradicate occupational fraud ought to put in place stringent compliance with regulations monitoring, frequent staff rotations to prevent collusion, technology to enhance tracking efficiency, employee lifestyle surveillance and ongoing instruction to enhance employee understanding and comprehension of rules and regulations. Financial executives should design antifraud methods that foster an ethical culture and encourage whistleblowers in order to increase revenue.

Ramadhan (2022) found that a variety of tactics can be used to increase fraud detection during COVID-19. The first tactic in forensic audits is to become more independent since this is crucial to doing audit tasks and because it forces them to decide for themselves whether or not the material they are using as evidence is sufficient, and free from outside influence. A forensics auditor's expertise in identifying fraud-related issues increases with their level of impartiality in reviewing audit facts or evidence. The next quality is objectivity; in order to avoid any conflicts of interest, forensic auditors performing audit assignments need to maintain a strong, unbiased position. This is due to the fact that objectivity is one factor that indicates the auditor is keeping the audit around in order to detect fraud during the COVID-19 epidemic.

The COVID-19 pandemic affected business processes on a global level presenting new risks for fraud and raising the rates of occupational fraud. This mass transition to remote employment, growth of the new communication platforms, and increasing popularity of online commerce brought new weaknesses that fraudsters could take advantage of.

2.3.1 Remote work and increased rate of fraud.

The shift toward teleworking at the onset of the COVID-19 pandemic created a number of difficulties regarding the systems of internal control in organizations. Sometimes standard safeguards including separation of duties were undermined since personnel assumed extra duties or ignored laid down procedures so as to ensure that organizations’ operations fully continued ACFE, (2021). Research shows that remote work conditions enabled staff to take advantage of oversight deficiencies primarily in areas that had not developed internal controls to work well under the new conditions Pwc, (2021).

As Button and Cross noted (2020), these vulnerabilities could be exploited resulting in occupational fraud including financial statement manipulation or misuse of company assets. This was so because during the initial weeks and months of the pandemic, many organizations had to keep operations running at the expense of orthodox anti-fraud measures.

2.3.2 Cybersecurity Threats

However, apart from the obstacles that were mentioned concerning remote working, cybersecurity issues escalated during the pandemic period. Increased levels of monetary and resource exchange through the internet, communication through interpersonal communication technology and the use of insecure networks exposed new windows for cyber fraudsters. The literature indicates an increase in phishing, malware, and ransomware in organizations which opened up new opportunities for engaging in occupational fraud Arner et al., (2021).

Research done by Anderson et al. (2021) show that firms need to enhance their security measures to protect against such threats. Businesses began to apply two-factor authentication, data encryption, and general staff education on how to avoid fraud after the COVID-19 outbreak. However, it was found that these measures produced the optimum results if implemented with speed and selectively depending upon the industrial segment that the organization belonged to.

2.3.3 Shifts in fraud precaution strategies before, during, and after the pandemic.

In the course of the pandemic, organizations have adapted their fraud prevention measures in order to counter threats. Some of the changes involved in managing fraud risks include revision of fraud risks management policies; strengthening of cyber security measures and innovation of other technologies like artificial intelligence fraud detection systems ACFE, (2021). Recent research about the aftermath of the pandemic suggests that while some of these measures worked in decreasing the level of fraud others are still being refined as organisations continue grappling with the changes that the pandemic has brought about to workplace fraud risks and dynamics Button & Cross, (2020).

2.4 Effectiveness of Modified Fraud Prevention Mechanisms

Zhu et al. (2021) examine how the pandemic has changed the characteristics of fraud risk and how different forms of data, such as unstructured and quantitative tabular data, have been utilised in fraud detection techniques. Basic quantitative data has evolved into the multi-source unstructured data that is employed in fraud detection procedures today. More information is available than ever in the post-pandemic age because of exploding data, and fraud detection tends to employ multi-source data to provide a complete picture of financial activity. Regarding the model, deep learning (DL) systems have gained popularity recently due to their adaptability and groundbreaking effectiveness in detecting financial fraud. An emerging method for analysing fraud activity data from multiple sources is graph-based detection. The swift advancement of technology has led to an increase in the complexity and intelligence of economic scenarios and behaviours. Since a graph may collect data from various sources to better simulate real-world activity and identify hidden deviations, graph-based detection techniques like GNN are gaining more attention. Even though data-driven DL models have shown to be useful in fraud detection situations, numerous issues need to be resolved before further advancement can take place. Galbraith et al. (2024) provided that numerous companies had to change their work environments—including employment, operations, and resource allocation—in order to recognise the pandemic's consequences. When these modifications were combined, they created incentives for workers to commit fraud. During the epidemic, there are some obstacles in the way of preventing and detecting fraud. These include questions regarding how the epidemic has altered the risk of fraud in addition to modifications to operating settings and investigation procedures. Managing the risk of fraud is crucial for preserving stability and liquidity as businesses continue to adjust to the post-pandemic workplace. Even though there are fewer reported fraud incidents, fraudsters' developing strategies and the shifting nature of remote employment necessitate ongoing awareness and preventative steps to guard against occupational fraud and associated dangers.

Grant Thornton (2021) provided that anti-fraud programs need to adapt to the significant changes in the corporate environment and processes brought about by the epidemic. The findings show that there are numerous chances for improvements in all organisations. For an organisation to be more effective after a pandemic, over fifty percent of respondents think that raising knowledge of fraud risk and fostering greater teamwork within the organisation are essential (53% and 52%, respectively). Just over a third of respondents listed just three areas as needing improvement: third- and fourth-party risk mitigation and due diligence; fraud risk awareness by third parties; and a change in emphasis from lagging to leading indications of risk. These findings imply that certain aspects of anti-fraud initiatives across numerous organisations need to be improved in order to make them more effective in the post-pandemic fraud environment.

Pulcine (2024) recommended that businesses should concentrate on strengthening internal controls, segregating duties, and monitoring financial transactions for effective fraud protection following the pandemic. Working together with specialists and fostering a vigilant culture are essential to preventing occupational fraud. In the post-COVID-19 environment, organisations that put an emphasis on internal controls and consult with forensic accountants will be better able to reduce risks. Wilasittha (2022) analyzes professional skepticism and the effect that applying remote auditing has on audit quality to establish how remote auditing should be implemented in the post-pandemic age. Using remote audits throughout the Covid-19 pandemic offers numerous benefits, including allowing the auditors to adjust to the use of technology in accounting auditing, saving money on audit expenses like travel and lodging, and enabling them to manage their time well enough to finish audits for multiple clients nearly simultaneously. However, notwithstanding the benefits, the auditor must continue to protect audit quality from a serious threat.

Copland (2021) stated that although pandemic-related fraud will eventually decline, the concept of being "always online" will not, which makes anti-fraud tactics and technology even more vital. Any company's first line of defence against fraud is its workforce. Nonetheless, fraudsters may take advantage of a staff member who is a weak link, so it's critical to make sure everyone on the team knows how to handle questionable activity. Employees should be aware that preventing fraud is a team effort and that each member has a part to play. Employees should feel free to discuss any doubts they may have with another staff member. Sari (2021) finds every indication of fraud in the financial statements of the local government following the pandemic. The findings of the data analysis utilising logistic regression analysis indicate that the fraud of local government financial accounts is influenced by pressure (financial stability and financial targets), opportunity (ineffective monitoring), competence, and arrogance. Concurrently, the findings demonstrate that collaboration, rationalisation, and outside pressure have little bearing on the falsity of local government financial statements.

Widiyati et al. (2021) discussed that the International Standard on Auditing (ISA), calls for the use of a risk-based auditing process, which can help public accountants (auditors) maximise their role in avoiding and identifying fraud in the taxation sector by ensuring that they carry out appropriate procedures that comply with useful auditing standards. In a risk-based audit, the auditor must identify risks by getting an adequate grasp of the business setting of the client, evaluate the risks that are found, and take appropriate action by implementing particular fundamental processes for the risks that are found in order to prevent either deceptive or fraudulent financial statements. Asset misappropriation with an effect on taxes or in general may be detected or stopped. Public accountants should focus on enhancing their individual autonomy, and tax authorities should implement Continuing Education Programs (PPLs) that teach accounting in compliance with current accounting standards.

In turn, as organisations carry on changing their fraud prevention measures in response to the COVID-19 pandemic, whether the altered measures are effective forms another research question. New technologies especially have been influential in changing the approach for prevention of fraud.

2.Technological innovations; these are the technological advances that have dominated most organizations and played a number of roles most of which are outlined below:

Among the many changes that have occurred in the management of fraud since the COVID-19 outbreak, the use of artificial intelligence and machine learning may be the most important. These tools have the ability for applying data mining techniques in real-time analysis of big data and distinguish between normal and suspicious activities that may involve fraud Schuchter & Levi, (2016). Blockchain has also been widely discussed as an effective technology that brings transparency and accountability to financial transactions and minimizes the risks of fraud Zhao et al., (2020).

Nevertheless, there are still some difficulties which can follow the indicated progress. In inadvertent cases, a powerful fraud detection system said Holtfreter (2015) is very efficient in its execution of scanning for possible frauds but at the same time the act results in high potentials for substantial false signals. Furthermore, the implementation of such technologies may also be very expensive especially for small organizations, and therefore they remain at greater risks of fraud.

2.4.1 Challenges in Implementation

Post pandemic fraud prevention also hinges on the organization's capacity to incorporate new technologies in their existing internal controls and risk management systems. This early sample of research shows that a blend of conventional and technological techniques may be the best defense against occupational fraud Smith, (2021). But more investigation has to be conducted to determine the long-term effectiveness of these strategies as the business environment changes.

This literature review maps out the development of fraud preventive measures from internal control and auditing to artificial intelligence-based fraud detection. Prior to the pandemic, these mechanisms were largely successful, though there were some lacunae regarding their ability to meet newer technologies and complex types of fraud. The pandemic brought new opportunities as well as threats: a higher likelihood of fraud in new remote work environment settings and significant cybersecurity threats. Research done after the pandemic reveals that technological advances have greatly enhanced the control of fraud; however, there are issues in the effective deployment of these technologies, and they are especially difficult to solve for small businesses. Since organizations are making several changes in the current techniques, they use in fraud prevention due to emerging new fraud tricks, more research studies need to be conducted in order to establish the extent to which such changes are effective in the current society.

2.5 Sector-Specific Fraud Prevention Approaches

Agwor (2017) concentrated on business "profitability, effectiveness, and efficiency" as performance indicators in manufacturing organisations, with a focus on fraud prevention as a component of the audit role. The study discovered that, in contrast to effectiveness and efficiency, which seem to have little bearing on the stated manufacturing businesses in Nigeria, fraud prevention has a more positive and significant impact on company profitability. In conclusion, firms tend to experience higher growth in terms of profitability the more stringently they avoid fraud. It is advised that businesses enhance their fraud prevention system to monitor any questionable behaviours in order to prevent fraud. According to the study, preventing fraud is a deliberate attempt to safeguard the company's growth, survival, and profit objectives because committing fraud undermines these objectives. Company performance when it comes to profitability tends to increase with the stricter fraud prevention measures. Omar et al. (2016)

examine the origins and effects of employee fraud in companies that manufacture automobiles, and suggest some preventive measures to reduce this unlawful activity. This study has offered several suggestions that the respondent company in particular, as well as the organisation in general, might implement to help reduce employee fraud. These include closely monitoring the work that the subordinate completes, training managers and staff on fraud awareness, creating clear job descriptions, creating a pleasant work environment, encouraging employee suggestions, tightening security controls, and posting friendly warning signs. Every day, cash must be deposited, and staff members are not permitted to spend their own funds on behalf of clients and then submit claims. Minimise the amount of float cash in the cash register. By regularly keeping an eye on the performance of subordinates and acting swiftly to address any signs of decline, management can lessen uncertainty.

Kankpang (2018) investigated how corruption techniques affected manufacturing companies' operating costs. According to the survey, fraud is an international problem that is wreaking havoc on economies and enterprises in both developed and developing nations. According to the study, the impact of corruption schemes on overall business costs is negligible, which goes against the a priori expectations. Enacting sufficient policies pertaining to personnel control at the highest levels of management is necessary to prevent fraud and misuse of funds. These policies should include job rotation, mandatory holidays and yearly vacations, privileges and restrictions, efficient oversight, strict and adaptable authorisation and approvals, and regular job rotation. Payroll-related methods in businesses should be as rare as possible by implementing strong checks and balances to guarantee that the payroll only includes those who are legally employed and working for the company.

Suh (2018) evaluates the connections between various fraud risk indicators and the perceived "opportunity reduction" in terms of the "likelihood of fraud occurrence" in financial institutions. The report recommended that the banking sector focus more on counter-fraud initiatives, which respondents to the poll identified as areas of weakness. To improve cooperation across the various financial industries and organisations for fraud prevention and identification, the banking sector should set up a centralised system for exchanging fraud data. The finance staff should be informed of the value of an ethical culture and personal integrity. Though it may seem a bit archaic, the most crucial basis for preventing fraud is personal integrity and an ethical culture. Furthermore, novice workers should not be allowed to become unintentional fraudsters by teaching them about the treacherous path that bank employees take to commit fraud. Mukah (2020) conducted a study to investigate methods for prompt identification and management of occupational fraud in Cameroonian MFIs. The empirical findings showed that in order for MFIs in Cameroon to effectively detect and control occupational fraud, they must: conduct regular monitoring and surprise audits; establish guidelines and notifications; avoid depending solely on accident and/or confession-related information to uncover occupational fraud; and finally, avoid relying too heavily on information technology control and surveillance due to the underdeveloped and highly politicised infrastructure that supports their operations in Cameroon. Therefore, it is imperative that all MFIs in Cameroon establish robust internal control systems and employ the four techniques suggested by this study to promptly detect and mitigate occupational fraud before it causes significant financial losses to the organisation.

Beemamol (2023) examined five prominent instances of high-value workplace fraud perpetrated by Indian bank executives at the upper levels of management. Numerous variables have been recognised as contributing variables, such as a hyper-competitive society, avarice, peer pressure, corrupt philosophy, a dearth of ethics and morality, arrogance, and a sense of entitlement and ego. These elements were crucial in persuading upper management to take advantage of fraud chances and work together with bank staff members and corporate debtors in order to further their own interests. An unsettling trend that puts the integrity of the banking sector at risk and may portend the industry's downfall is the frequency of collusive fraud.

Akuh (2017) examined the methods employed by a few managers and small retail business owners in order to identify and stop employee dishonesty. The data gathering revealed five primary emergent themes including "cash register accountability, controls and communication, segregation of roles, monitoring and taking action against offenders". Increased adequate controls against employee fraud and the chance for small retail enterprises to run profitably and successfully are two potential positive social change consequences. These could lead to an increase in employment opportunities. The main conclusions of this study were that managers and owners of small retail firms must use techniques to identify and stop employee fraud. The results of this study may also be used to better inform managers and owners of small retail enterprises, both current and prospective, on the significance of creating, preserving, and keeping an eye on effective internal controls. Alcobary (2022) examines the tactics employed by retail industry leaders to deter and lessen employee theft. Three themes emerged from the participant data in relation to employee theft. The themes that were found include "internal control and monitoring, responsibility and task separation and assembling a devoted and accountable team". The results of the current study suggested that business executives may be able to avoid and lessen employee theft if the recommended measures are successfully implemented. Positive social transformation and business practices have the potential to reduce financial loss and business failure for merchants, increase employment, support long-term business continuity, and improve the financial condition of local residents.

Matagaro (2018) determined the elements impacting the risk of occupational fraud in retail chains. The results of the study showed that corporate management affects the risk of occupational fraud. Thus, the study comes to the conclusion that a high likelihood of professional fraud risk might be created by incompetent management. By keeping an eye on management oversight and striking a workable balance between the distribution of resources and occupational fraud exposure, the retail chain industry can gain some justifiable benefits in lowering occupational fraud. Furthermore, it is clear that an industry can suffer greatly from staff members having disproportionately high levels of trust; for this reason, managerial regulations and procedures should always be followed. The investigation comes to the conclusion that workers committed fraud because they were living beyond their means. The study also showed that employee attitudes can shift significantly, particularly if they are dissatisfied with their jobs or are underpaid, which can lead to possibilities for occupational fraud.

Obiora et al. (2022) examined how forensic accounting can help in fraud prevention in the context of healthcare firms in Nigeria. Based on the statistical examination conducted, the report deduces that forensic accounting firms can effectively uncover fraudulent activities and fraud in Nigerian healthcare organisations. Forensic accounting is therefore regarded as a tool for preventing fraud amongst the Nigerian enterprises that have been quoted. As a result, the study suggests that a sufficient system of internal controls be put in place to have personnel oversight and decrease fraud to the barest minimum, giving prospective and actual investors their confidence back. Additionally, as Nigerian healthcare workers play a crucial role in preventing fraud, their well-being and compensation ought to be given careful consideration. Griffin (2017) conducted a study to elaborate on the numerous difficulties in preventing healthcare fraud. The degree of fraud committed by medical professionals and non-medical individuals was made clear by the study findings. The government's dearth of internal controls allowed this kind of fraud to go unnoticed for a long time, costing tens of millions of dollars annually, as the analysis also discovered. While there are new technologies available, fighting healthcare fraud will require cooperation between "the federal, state, and local governments".

As a result, fraud prevention measures differ within the courses of their distinctive operational features and risks each sector has. In this section, we explore fraud prevention approaches within three key sectors: business sectors including; financial services, retail and manufacturing. Fraud risks are ubiquitous in each element of the organization and require specific approaches to minimize the threat appropriately. Knowledge of these industry-specific measures can help to get an idea about how organizations may construct and develop fraud prevention measures to confront their special risks.

2.5.1 Financial Services

The financial services industry remains at a high risk for occupational fraud because of issues such as the complexity and value of its transactions, the presence of regulatory requirements, and operations' dependence on technology. This sector also suffers some of the steepest regulatory rules in areas such as fraud prevention. In light of this, financial institutions have enhanced the means by which they prevent fraud that seeks to compromise the financial institution.

The most popular measures in the financial services industry are based on the application of advanced IT tools, including AI and ML technologies. It allows those in the financial industry to account for a high number of transactions as they take place, and anticipate any behaviour or activity that should raise suspicions of fraud. As suggested in the study by Ryman-Tubb et al. (2018), the systems with AI enable it to recognize the patterns of behavior, provide the warning of the specific activity, for example, large transactions, and minimize fraud potential. It is most appropriate in the identification of fraud including identity theft, insider trading and unauthorized transactions common in financial related firms.

The other chief strategy that is largely significant in tackling fraud incidence is regulatory compliance. Banks and other financial businesses are aware of several anti-fraud legislations; these are the SOX, the FCPA and AML laws Krause, (2017). Implementation of these regulations makes it necessary for financial institutions to put in place stringent internal measures, carrying out periodic and independent examination of records, and provide reports of suspicious activities to the authorities. A number of organizations have implemented a "three lines of defense" approach, where; the first line is the operating management and performing initial fraud detection on a daily basis; the second line is the compliance and/or the risk management; and the third line is the internal and or/external auditors IIA, (2021).

However, even with these and other standard precautions in place, the allied areas of financial services still remain highly susceptible to fraud, more so based on virtual and or cybercrimes as well as through increased embrace of digital payment platforms. This means that fraudsters are getting more and more creative with their ways to get around the regular checks. Consequently, there is a constant need to upgrade various technologies or sustain and even enhance state-of-art fraud prevention approaches Krause, (2017).

2.5.2 Retail

The retail industry too has its separate set of issues when it comes to fraud prevention because of which they have a large number of transactions which increasingly are in different forms of payments and also are shifting more of the retail business online. Some of the retail fraud common in retailing are; Return fraud, credit card fraud, theft and manipulation of POS systems. To tackle such fraud risks retailers ought to employ a variety of solutions that both include use of technologies and staff training in order that fraud is addressed as soon as it starts happening.

The most implemented anti-fraud measures noted across the retail business are sophisticated POS systems with functionalities for fraud detection. These systems track transactions in real-time, look for irregularities in buyers' behavior, and report doubtful transactions. In a report by PricewaterhouseCoopers (PwC) (2021), POS systems in retail companies who adopt AI-based fraud detection tools have experienced drastically low transactional fraud especially with credit card payments. These systems can identify some sequences that indicate the use of such credit cards as fake and bring the operation to a stop before fraud occurs.

But, the advances in e-commerce utilization in the retail business increase new fraud risks. Other types of retail fraud that have grown with the increased uptake of internet sales include CNP fraud and account swimming. To address the problem, retailers have adopted defense measures that include multi-factor authentication, encryption and tokenization technologies to protect the customer data and curb fraudsters Nilsson et al., (2021). The firm has successfully implemented these innovations for minimizing the risk of fraud on its internet operations even if constant enhancement is an ongoing process due to the emergence of new risks.

2.5.3 Manufacturing

While manufacturing is not a sector with highly indicated fraud risks compared to sectors like financial services and retail, manufacturing risk exists, often in procurement and inventory fraud, financial statement fraud, etc. Manufacturing operations are complex with dispersed operations in supply chains and vendor networks and they offer numerous chances for fraudsters to implement blunders in internal controls.

A major strategy of fraud prevention unique to the manufacturing industry is normally the use of strict purchasing checks. Among all the fraud types, procurement fraud, which often involves kickbacks, bid-rigging and invoice fraud, ranked one of the most common in this industry ACFE, (2021). Manufacturers manage this risk through clear sourcing practices, creating strict information systems to track supplier transactions and have stringent check-ups of the relationships with suppliers. An efficient strategy to mitigate fraud risk is considering that different people perform procurement contracts’ approval, managing relations with suppliers and payments’ processing Tepalagul & Lin, (2015).

Another reason associated with the utilization of inventory management systems is to eliminate fraud among manufacturers. These systems assist in tracking stock of raw materials and finished products to assist in the preparations of account balances and to prevent and detect cases of embezzlement of stocks and falsification of records. Real-time inventory tracking through RFID and other methods like barcodes will help manufacturers understand that there is a problem in their stock counting process since it is easier to monitor it and control fraud Quesenberry, (2016).

In general, manufacturing firms continue to experience reduced rates of fraud compared to other industries, but they are at risk given the strenuous procurement supply and the high-value products manufactured. Controlling these risks involves coming up with sound controls and always assessing processes and procedures in regards to these risks.

2.6 Departmental Fraud Prevention Strategies

Peicheva (2012) gives evidence to back up the claim that the HR department is crucial to preventing fraud. The Human Resource Department plays three key responsibilities in fraud detection and prevention: "architect," "observer and analyst," and "knowledge distributor." Two requirements must be satisfied in order to perform these roles. The Department of Human Resources plays a crucial role in preventing fraud, so the corporate management should first set up the right environment for it to do so. Secondly, personnel working in the Human Resource Department ought to possess extensive training to effectively perform their duties related to preventing fraud. If these requirements are not met, we will continue to examine the same fraud-related facts in the future. Lowers (2015) discussed that managers are at the forefront of the fight against fraud within organisations. The best defence from fraud is prevention, and hiring competent people is the best way to take preventative measures. Risk experts utilise a model called the Fraud Triangle to describe fraud in the workplace. According to the model, there was an opportunity, an incentive, and an employee's rationalisation for engaging in fraud. HR managers are in an exceptional position to understand and solve each of the two legs of the triangle, even though risk managers usually have the greatest influence over the opportunity component via different controls. They can discover the views, attitudes, and expectations of employees by doing suitable training, testing, and observation.

Ilmiha and Suboh (2024) examine how well internal control works to stop accounting fraud in financial institutions. The study's findings demonstrate the critical role that thorough risk assessment and a robust control system play in lowering the likelihood of fraud in accounting. The study's result verifies that a system of controls that effectively prevents accounting fraud in financial institutions must have good integration between its numerous internal control elements. Fraud detection and prevention depend heavily on the "finance department, internal audit, and top management" having open and efficient communication. Businesses with improved departmental communication have better fraud detection rates. Kaur et al. (2023) determine the role that forensic accounting plays in the identification and avoidance of fraud. Forensic accounting and fraud detection and prevention are positively correlated. Furthermore, the authors indicate that fraud is complicated and that one needs to be conscious of this complexity while conducting investigations into fraud in regard to empirical and non-empirical findings. The main things impeding forensic accounting are ignorance and training. Forensic accounting must therefore be included in both courses for undergraduates and graduates.

Kashona (2019) examines how well the Ministry of Finance's internal audit system detects and prevents fraud. The study's findings demonstrated that the MoF had internal inspection and control procedures. Internal control and effectiveness of internal audits, however, could be characterised as ineffective due to management's failure to act upon the conclusions and suggestions of internal auditors. Fraud incidents are rare among government ministries with strong internal control and internal auditors. The investigation also finds that the MoF's internal control and internal auditors provided an unbiased assessment of the MoF's activities, that the MoF did not provide the auditors with official audit education, and that the auditors were given skills appropriate for their position in the MoF's internal audit division. According to the report, MoF leadership should purchase the newest ICT internal audit program to ensure improved risk assessment and enhance the provision of services, particularly fraud detection and non-compliance management. As mandated by the Institute of Internal Auditors and professional associations like the "World Bank and the International Monetary Fund", internal auditors ought to be routinely exposed to advancements in auditing frameworks. Chibuike (2023) discussed that in the public sector, oversight of finances is crucial to preventing fraud and misappropriation of funds. "Segregation of roles, internal controls, audit trails, and training and awareness" are examples of effective financial control methods that can assist organisations in upholding regulatory compliance, openness, and public trust. Public sector organisations can guarantee responsible management and appropriate use of taxpayer funds by putting these procedures into place. Organisations in the public sector have an obligation to uphold the strictest guidelines for accountable and efficient fiscal oversight. Financial theft and improper use of funds can have serious repercussions, including a decline in public confidence, legal action, and harm to the image of the organisation.

Hassan et al. (2023) examine how internal and external auditors, as well as financial accountants, view the relationship between IT and corporate governance (CG) and how they affect the identification and prevention of fraud in businesses. The findings show that effective CG procedures and IT strategies greatly assist in identifying and lowering fraudulent activity by lowering the chances, justifications, pressures, and capacities of prospective workers to commit fraud. Internal measures have also significantly decreased fraud incidents. Particularly, ethical officers and training on ethics were not thought to be highly helpful in stopping and identifying fraud, which increased the likelihood of more fraudulent acts in the future and gave rise to the impression that fraudulent behaviours are common. According to this study, strong CG procedures should be implemented in order to spot possible fraud within an organisation. Furthermore, for optimal use, IT techniques must be customized to particular requirements.

Suryanto (2016) examines how information technology, financial reporting, and dividend policy affect the avoidance of fraud. Information technology has a demonstrated impact on preventing fraud. Information technology deployment that supports enterprise IT activities in producing accurate information has a significant positive impact on preventing fraud (fraud) inside enterprise organisations. In order to boost confidence among shareholders, a business must be able to demonstrate strong business performance and provide investors with sufficient updates on the company's progress. Before making an investment, both current and prospective investors should research the business profile and the information provided by the issuing company to see if it satisfies the information requirements of the financial analysis.

Preventing fraud is an organizational initiative as well as a departmental undertaking because each department in an organization is vulnerable to different fraud risks hence comes with its measures. This section explains and discusses the nature of how corporate departments like finance, HR and IT come up and put into practice fraud preventive measures against either internal and external fraud threats.

2.6.1 Finance Department

The finance department should be considered the most important in combating fraud in an organization since it handles all the financial resources, payments and the provision of financial reports. E-mail and payroll fraud pose big risks, and the financial fraud, including embezzlement, payroll and/or financial statement fraud also presents the major risks which necessitate internal controls amongst the finance department.

One of the oldest methods of preventing fraud within the finance department is the separation of responsibilities. Separating responsibilities makes certain that one worker is not authorized to perform a number of functions within a financial transaction, namely issuing, posting, and scrutinizing checks Albrecht et al., (2012). This helps minimise cases where some persons may compromise transactions or embezzle funds with no easy way of being caught. To prevent and identify the tendency of financial fraud, financial departments use standard and non-standard internal and external audits. The study done by Rezaee and Riley in 2019 revealed that organizations that undertake frequent financial audits are less likely to be hit by fraud as the auditors are in a position to detect early signs of fraud and make the necessary recommendation.

Further, finance departments use technology to enhance fraud control measures they employ in their institutions. Financial transactions can be closely monitored since they are processed by automated systems thus the detection of fraudulent activities is easy. There are more and more computerized techniques in the detection of fraud indicators in financial statements and in other types of transaction processing, making it very difficult for fraud to go unnoticed Holtfreter, (2015).

2.6.2 Human Resource Management Department

Human Resources cut a lot of effort by ensuring that dominated employees as well as those who are hired and retained have to conform to ethical practices as a way of preventing fraud. With regards to fraud prevention in the human resource department, proper screening works include background checks, reality of references, and criminal history checks before employee hires. The study conducted by KPMG in 2020 proved that the firms conduct the background check to ensure they minimize on recruiting employees with records of unethical behavior, which decreases the internal fraud rates.

This is also because HR departments are also involved in fraud control by promoting a sound ethical culture within the organizations. This may be done through implementing policies such as offering sensitivity training for an organization's employees with aims at making the employees understand the various risks that they are exposed to concerning fraud and why internal controls are important Zhang et al., (2019). This also means that HR departments should also ensure that whistleblower policies to be used by the organization for employees to report suspicious activities without the fear of being fired are instituted. Wells (2017) postulates that efficient freedom of whistleblowers is an essential part of the organizational procedures of anti-fraud and correlates with the scheme of 'first responders.'

2.6.3 IT Department

As the first line of defense of technology fraud, especially computer crimes, theft, and system manipulation, IT is on the frontline in guarding against such incidents. In today's business environment, various organizations operate within digital environments, and the IT department plays the role of an information security officer to prevent the leakage of information.

Currently, MFA, encryption technologies, and other optimal measures have become one of the most widespread practices in the IT department dedicated to fraud prevention. MFA ensures users receive extra protection additionally in terms of password authentication for it allows two or more methods of the same account before that account can be granted access to certain systems or information. From the work of Anderson et al. (2021), it is clear that organizations that have adopted MFA are less likely to be attacked through some of the most common techniques used in cyber fraud. It also guards sensitive data in a way that only authorized users can access it since the data is encrypted.

Other responsibilities of IT departments include that of surveying activities of systems for any sign of fraud. With the help of real time monitoring tools, IT employees can outline the activity which looks suspicious, for example, attempts of unauthorized access or deviations from regular data processing and respond to fraud threats without delay Holtfreter, (2015). Daily system scans and vulnerability scans also point out an organization’s particular susceptibilities within its information technology structure that the IT department can fix before becoming a target of fraudsters Quesenberry, (2016).

Likewise, having individualistic strategies in place, different departments of one organization apply various measures to prevent fraud risks: the finance department deals with audit of financial records and structural separation of various responsibilities, the HR departments underline the importance of proper checking of employees with the help of strict programs and motivation of whistleblowers, and at last, the IT departments are aimed at cybersecurity. Taken collectively, these sector/integrated and departmental strategies constitute a rather systematic approach to addressing occupational fraud risks.

2.7 Impact of Company Size on Fraud Prevention

Sari et al. (2023) examine the relationship between fraud within Sharia banks and "Sharia compliance, Islamic corporate governance, and company size”. The study found a positive relationship between internal fraud and company size. Moore (2016) ascertains whether the incidence and degree of occupational fraud are correlated with the size of the organisation. The findings of this study indicated there is a connection between organisational size and the rate of incidence, and severity of, professional fraud. The results suggested that occupational fraud disproportionately impacts smaller enterprises more than it does larger ones. One suggestion for more research is to use data from organisations outside of the United States in the study. Shao (2016) implied that an efficient internal control system which makes use of both preventative and investigative internal controls must be built in order to stop fraud from happening. This framework will serve as the cornerstone for recording transactions and making business choices. Because internal control mechanisms have a tendency to malfunction over time, it is also necessary to continuously monitor this one. When combined, these broad internal safeguards and the other controls suggested in this thesis can lessen asset theft and aid in the early discovery of fraud, preventing losses for small businesses before it's too late.

Mariner (2020) looks for any connections among the number of staff members and the extent and prevalence of occupational fraud in small enterprises. The incidence of occupational fraud and the total number of staff members in small enterprises were found to be statistically significantly correlated in the present investigation, with a p-value of 0.02. With a significance level of 0.104, the results also revealed no statistically significant relationship between the number of workers and the degree of occupational fraud in small enterprises. It was implied that segregating duties could be a more economical way to tackle occupational fraud in the United States. Sow et al. (2018) discussed fraud prevention in the context of small enterprises. The analysis went on to show that Malaysian SMEs have taken a few steps to prevent fraud in order to lessen the expensive illicit operations that endanger their long-term viability. Among Malaysian SMEs, creating a positive work environment was determined to be the most widely employed fraud prevention strategy. Conversely, the least effective strategies were creating an internal audit or fraud investigation department, hiring an outsider, such as qualified fraud investigators or outside auditors, and providing fraud awareness training. The most successful strategies were thought to be consistent in responding to fraud cases that were reported, creating a positive work atmosphere, creating an auditing department, implementing internal control, and raising management's awareness of fraud risk.

Gunasegaran et al. (2018) determine the scope and nature of the fraud plan, the safeguards in place, and the difficulties facing Malaysian medium-sized businesses. The results imply that non-cash larceny and damaged trust were connected to the fraud incidents that the businesses encountered. Because of financial and resource limitations, there doesn't seem to be much use of fraud protection techniques in businesses. The study's conclusions carry worrying implications for the directors and owners of the chosen medium-sized businesses. They don't appear to have taken the same proactive approach as larger organisations, but they have implemented fraud prevention procedures in response to fraud within their organisations. Due to this circumstance, the business may be at risk of losing its ability to compete and endure in the market. Alayli (2022) contested that SMEs are significantly more likely to have staff losses than major firms, and they are also far less probable to be able to withstand these losses. Compared to large businesses, SMEs are more adept at managing internal control. Monitoring tools are desperately needed by businesses in the modern day, since recent research indicates that monitoring frameworks have an impact on performance reviews. The managerial mindset of a corporation is shaped by the environment in which it operates. The monitoring system serves as the framework for adding additional levels of internal control. As a result, the subjects of the research cover the work environments and cultures of the organisations as well as the ethics and moral convictions of the staff members who design and implement controls. An ecosystem needs the interaction of numerous components to remain stable.

Daraojimba (2023) discussed the challenges associated with financial fraud prevention. The study suggested that forensic accounting appears to have a bright but difficult future. It is anticipated that fraud detection capabilities will be greatly improved by the growing integration of technology like artificial intelligence and predictive analytics. However, there are drawbacks as well, such as the requirement that forensic accountants pick up new abilities and adjust to quickly evolving technology environments. Because digital financial fraud is always changing, forensic accounting procedures will need to remain creative and vigilant. Oladejo and Jack (2020) examine the difficulties that blockchain presents for forensic accountants who work in the field of fraud prevention and detection. Based on the existing literature, blockchain has the capability to prevent and safeguard against fraudulent activities due to its utilization of cryptographic signatures, distributed ledger, and P2P network. It is acknowledged in this research that blockchain cannot ensure the authenticity of source documents as the input determines the output. Despite the presence of preventive technological measures such as cryptography and P2P networks, it is acknowledged that the technology is not completely immune to malicious attacks and hacking. This study reinforces the idea that both human and technical factors, which impact fraud prevention and detection systems in other e-commerce innovations, could also affect blockchain technology, as the human element remains the weakest link in any system. Consequently, if source documents are vulnerable, the output might not be dependable.

Śmiałek-Liszczyńska (2023) makes suggestions for SMEs looking to lower their risk of occupational fraud. Although there is always a chance of fraud in the workplace, there are steps that may be taken to reduce the risk. For example, changes in internal processes or job rotation might lead to the accidental discovery of fraud cases, even ones with the highest financial cost. The decisions made by managers and business owners have a significant impact on how their employees behave. Hard recommendations, which are classified as low-cost, include things like facilitating fraud reporting channels, putting procedures in place for the most crucial processes, regularly analyzing and verifying data, and setting reasonable targets for staff members. Hard steps are inexpensive in comparison to the extent of the repercussions of deception. Naturally, a business needs to be able to use the tools in relation to the work that its workers perform and the expenses associated with doing so. The price of not taking the necessary precautions to stop fraud may exceed that of taking such precautions. Ortiz-García (2022) examines the tactics employed by certain proprietors of small eateries to lower the incidence of occupational fraud. The study's conclusions suggested four tactics to lessen employee fraud. These include analytical processes, owner oversight, task segregation, and efficient staff communication. In order to put these methods into practice, participants identified important factors that business owners should take into account. Using relatives, internal audits, and surveillance devices are crucial components of a successful owner's surveillance program. The application of analytical techniques and a sufficient division of labor for cash, inventory, and sales transactions were also mentioned by those surveyed. Owners may take into account internal memoranda, procedure manuals, and written policies for their communication approach. Business executives and other professionals can use the study's results to lower occupational fraud, boost revenue, and foster community trust—all of which will benefit society in its entirety.

Macaulay (2020) suggested that understanding and comprehending the meaning and signs of occupational fraud provides the internal auditors with adequate direction and advice needed to efficiently carry out and carry out value-adding services that aid the organisation in avoiding, identifying, and reducing occupational fraud schemes. This is because fraudsters are constantly evolving in their "technical expertise, strategies, complexities, and technological skills in order to exploit power, influence, opportunities, and organisational resources" for personal satisfaction and professional advantage. By properly observing behavioural and organisational indicators acquired from numerous fraud research studies as well as via actual evaluation and investigation of fraud instances, unlawful activities may be exposed.

The type of failure has a clear impact on the capability of a firm and their fraud prevention measures. As is evidenced by the information presented in this paper, the issues that SMEs and large companies encounter when addressing fraud prevention vary significantly because of the differences in the amount of resources, existing internal controls, and organizational structures. Knowledge of some of the dynamics of Company size and its fraud prevention measures are very vital when preparing anti-fraud measures which fit an organization's needs best.

2.7.1 Small and medium-sized enterprises' fraud prevention

Occupational fraud is often prevalent amongst SMEs because such companies can rarely spare much of its budget towards the prevention of fraud. In its report, the Association of Certified Fraud Examiners (ACFE) (2021) noted that SMEs are more severely impacted by fraud as compared to larger organizations, due in large to a poor implementation of strong internal controls, like separation of responsibilities, or robust working audit checks. For instance in many SMEs, different layers of a single transaction may be handled by the same employee thereby exposing the business to the risk of fraud that may not be easily detected Wells, (2017).

Besides, SMEs are less likely to have personnel for fraud prevention and control, fraud detection instruments such as those developed based on AI and ML that are regularly used in large establishments Ryman-Tubb et al., (2018). SMEs usually adopt a policy control and the supervision of the managers in which they are limited in comparison with the formal control and are not very effective for the identification of the complex frauds Peltier-Rivest & Lanoue, (2015).

Sound procedures that can be adopted by SMEs include; conducting efficiently inexpensive control measures like the vigorous background checks on employees; developing and putting into practice an efficient working policy for whistleblowers; and engaging the services of external auditors to carry out a periodic scrutiny over the SME's financial records and statements. Further as pointed out by Zhang et al., (2019), SME owners and managers should be closely involved in the monitoring of financial transactions as it has been seen to act as a deterrent to fraudulent conduct. SMEs have low resources, but they should quickly analyse fraud risk and create an environment based on accountability and transparency.

2.7.2 Large Corporations Fraud Prevention

The fraud fighting mechanisms in large corporations are more well developed than in the small ones because the former has more resources and powers, number of employees and use of advanced technologies. They can bear the cost of ‘state-of-art’ fraud prevention measures like artificial intelligence analytics that constantly scan huge numbers of transactions for fraud and alert when something is suspicious Schuchter & Levi, (2016). Furthermore, large organisations especially have well defined internal controls, ending with documented policies and procedures, segregation of roles and responsibilities, internal and external audits among others Albrecht et al., (2012).

But even then, large corporations present a unique set of factors that make it difficult to prevent fraud. The complexity of their operations, size of the number of employees and branches they have spread in makes it hard to prevent collusion fraud Free & Murphy, (2015). Moreover, a large number of transactions and departments also create a problem of recognizing the fraudulent undertakings on time. This is why large corporations utilize multiple fraud risk management layers-including fraud risk management team, data analytics, and external fraud audits-into strengthen their detection systems Pope & Lee, (2019).

These best practices entail constant scrutiny of transactions and immediate analysis, additionally training of employees concerning susceptibility to fraud in organizations particularly’ large corporations. Through the utilization of its resources to develop extensive fraud preventive measures, the big businesses are in a better position to fight occupational fraud.

2.8 Research Gap:

The formation of vulnerabilities for fraud can be caused by the occurrence of a financial crisis and the company's working conditions being different from normal during the epidemic Wulanditya et al., (2022). The coronavirus disease 2019 pandemic has hastened the digital transition and brought about unforeseen economic downturns, which have strengthened financial fraud motives and made fraud schemes more intricate. Despite the fact that academics, practitioners, and regulators have started to concentrate on the novel aspects of financial fraud, a methodical and successful anti-fraud approach throughout the pandemic still needs to be investigated Zhu et al., (2024). Dias (2021) suggested that in order to determine the elements that can result in fraud in commercial corporations, banks, public institutions, small and medium-sized businesses, and other sorts of organisations both qualitative and quantitative analysis studies should be conducted on these types of organisations as potential future research routes. In the end, it would be fascinating to observe what happens to these models in the present following a pandemic, which will have a significant influence on society because of the social and economic ramifications that will be felt by businesses and employees. Considering these gaps, this study aims to comprehensively investigate and analyze whether organisations have modified their existing fraud prevention mechanisms to mitigate the chances of occupational fraud and to understand the factors influencing these modifications, with a focus on post-pandemic adaptations.

The literature review identifies a major research gap related to the relative efficacy of anti-fraud measures in organizations of various types and sizes. To the authors' knowledge, prior research has established fraud prevention mechanisms but has not done so comprehensively, systematically, or comparatively regarding the difference between SMEs and large corporations or between organizational departments. Secondly, although COVID-19 has disrupted many businesses, little is known regarding its influence on fraud prevention contingency plans and how organizations have changed their strategies to implement new fraud risks.

By undertaking a comparative analysis of the preventative measures implemented in different organizations of different sizes and from different sectors, including how these measures have been changed since the onset of the pandemic, the current study seeks to fill this gap. Also, the study will determine the cross-department application effectiveness of the strategies and possibly compare or contrast the sector specific approaches.

2.9 Research Hypothesis:

H01: There is no significant difference in the utilization of fraud prevention mechanisms across various departments within organizations.

H02: There is no significant difference in the modifications made to fraud prevention mechanisms post-pandemic across organizations.

H03: There is no significant difference in the effectiveness of fraud prevention mechanisms across various departments, both pre-and post-pandemic.

H04: There are no commonalities and differences in fraud prevention approaches employed by organizations in different sectors and sizes.

Its elaborations:

H01: There is no significant difference in the utilisation of fraud prevention mechanisms across various departments within organisations.

H11: There is a significant difference in the utilisation of fraud prevention mechanisms across various departments within organisations.

H02: There is no significant difference in the modifications made to fraud prevention mechanisms post-pandemic across organisations.

H12: There is a significant difference in the modifications made to fraud prevention mechanisms post-pandemic across organisations.

H03: There is no significant difference in the effectiveness of fraud prevention mechanisms across various departments, both pre and post-pandemic.

H13: There is a significant difference in the effectiveness of fraud prevention mechanisms across various departments, both pre and post-pandemic.

H04: There are no commonalities and differences in fraud prevention approaches employed by organisations in different sectors and sizes.

H14: There are commonalities and differences in fraud prevention approaches employed by organisations in different sectors and sizes.

2.10 Summary

This research aims to explore if the organisations have modified their existing fraud prevention mechanisms to mitigate the chances of occupational fraud and to understand the factors influencing these modifications, with a focus on post-pandemic adaptations. Considering these aims, this chapter first discussed the theories associated with the study focusing on the Fraud Triangle theory and The Fraud Diamond Theory. Following this, the study discussed the fraud prevention mechanism before the pandemic, focusing on the studies that were conducted before the pandemic on this subject. Furthermore, the section then discussed the risk associated with fraud during the pandemic while focusing on the changes in fraud prevention measures during and after the pandemic. The next section evaluates the changes in fraud prevention effectiveness after the pandemic. The section reviewed the studies that describe the role of technological innovations in fraud prevention. The next section outlined the sector-specific fraud prevention approaches. This includes discussion on fraud prevention in manufacturing, retail, finance, healthcare sector etc. The next section discusses how different departments approach fraud prevention. Finally, the influence of company size on fraud prevention was discussed. The chapter concludes by outlining the research gap and research hypothesis. In the next chapter, research methodology will be discussed focusing on different choices made by the scholar to fulfill the research objectives.

This chapter has discussed works done previously regarding the fraud prevention mechanism, such as the sector wise and department wise strategy, role of size of the company and changes due to COVID-19 pandemics. The review noted a specific research void concerning relative efficacy of fraud prevention tactics in various organizational settings, an issue the present investigation seeks to fill. The hypotheses given in this section will provide the basis for empirical analysis, which will help to identify differences in fraud prevention activities between departments, sectors, and companies' sizes and analyse how these practices have changed after the start of the COVID-19 pandemic.

CHAPTER III: RESEARCH METHODOLOGY

The research methodology chapter is a crucial component of any academic study as it outlines the systematic process followed to conduct the research. This chapter not only explains the methods and techniques used for data collection but also justifies their appropriateness in achieving the research objectives. In this discussion, I will delve into the research methodology chapter and its implications in the study, with a focus on the utilization of different research instruments to achieve the research objectives.

The research methodology chapter typically consists of several subheadings that provide a comprehensive understanding of the methods employed in the study. These subheadings may include "Research Design," "Data Collection Methods," "Data Analysis Techniques," and "Ethical Considerations." Each of these subheadings plays a pivotal role in shaping the overall research methodology and contributes to the credibility and validity of the study.

The choice of research instruments is a critical aspect of the methodology chapter. Research instruments refer to the tools and techniques used to gather data and information for the research. These instruments can vary widely depending on the nature of the study and the type of data required. Common research instruments include surveys, interviews, questionnaires, observations, and archival research, among others.

To achieve the research objectives effectively, a combination of research instruments may be utilized. For instance, if the research aims to explore the perceptions and experiences of a specific group of individuals, a mix of interviews and surveys could be employed. This approach allows for a comprehensive understanding of the research topic by capturing both qualitative and quantitative data.

Furthermore, the research instruments should align with the research questions and objectives. The rationale for selecting a particular instrument should be clearly justified in the methodology chapter. This justification involves discussing the strengths and limitations of the chosen instruments and explaining how they contribute to answering the research questions.

Additionally, the methodology chapter should address the reliability and validity of the research instruments. Reliability pertains to the consistency and stability of the instruments in producing accurate results, while validity refers to the extent to which the instruments measure what they are intended to measure. Discussing the steps taken to ensure the reliability and validity of the research instruments demonstrates the rigor and robustness of the study.

Moreover, ethical considerations associated with the use of research instruments should be addressed in the methodology chapter. This includes obtaining informed consent from participants, ensuring confidentiality and anonymity, and adhering to ethical guidelines and regulations.

In conclusion, the research methodology chapter serves as the roadmap for conducting the study and holds significant implications for the research. The selection and utilization of research instruments play a vital role in achieving the research objectives and generating reliable findings. By carefully outlining the research instruments and justifying their appropriateness, the methodology chapter enhances the credibility and trustworthiness of the study.

3.1 Overview of the Research Problem

Organizations around the globe are at risk of occupational fraud. As defined as the purposeful violation of stated policies and regulations for one's self benefit through fraudulent activities, it may assume different guise, such as embezzlement of assets, fraud in financial statements, and corruption. ACFE noted that while fraud situations differ by country, international studies show that organizations lose about 5% of their annual revenue to fraud ACFE, (2020). Given the increased intricacy in business organizations and the growing adoption of Internet-based systems, occupational fraud is not only more diverse but also much more difficult to identify. Occupational fraud affects an organization in terms of financial loss and its image and the well-being of its employees. There is a need to put in place measures that help control fraud risks in an organization since these are some of the major risks facing an organization. However, the usefulness of such mechanisms is influenced by several factors such as size of the organization, industry type and issue nature confronting different departments.

It can be recalled that anti-fraud measures are designed to detect, discourage, and prevent fraud in organizations. Organizational antifraud resources implemented by various departments appear to have specifically prescribed responsibilities in combating occupational fraud. For instance, a company's HR department may be responsible for running background checks in relation to employee screening, whereas accounting and finance perform controls such as separation of duties as well as monitoring of transactions. The IT departments impose security measures to safeguard confidentiality and prevent loss of proprietary information. Specific tools that are used with financial transaction analysis include, but are not limited to real-time transaction monitoring in banking industry or compliance software in industries such as healthcare Kroll, (2022).

Although these mechanisms are common in pretty much any organization, their efficiency greatly depends on the relative expertise of the department in question, technology programming, and organizational culture overall. I have just highlighted that the biggest issue relates to this dynamic and, therefore, the need to evolve and strengthen resistance against fraud all the time; With safeguards such as physical security or manual audits proving to be ineffective since fraudsters are shifting their focus to take advantage of digital risks., including asset misappropriation, financial statement fraud, and corruption. The Association of Certified Fraud Examiners (ACFE) estimates that businesses lose approximately 5% of their revenue annually to fraud, resulting in substantial financial losses ACFE, (2020). With the complexity of business operations and the rise of digital platforms, occupational fraud has become more sophisticated and harder to detect. Occupational fraud impacts not only an organization's financial health but also its reputation and employee morale. Implementing effective anti-fraud controls is a priority for organizations seeking to minimize these risks. However, the effectiveness of such mechanisms depends on several factors, including the organization’s size, sector, and the specific challenges faced by different departments.

Fraud prevention mechanisms aim to identify, deter, and mitigate fraudulent activities before they occur. Different departments play distinct roles in preventing occupational fraud. For example, HR may focus on background checks and employee vetting, while accounting and finance departments implement internal controls like segregation of duties and transaction monitoring. IT departments enforce cybersecurity protocols, ensuring data integrity and preventing unauthorized access. In industries like banking or healthcare, specialized tools such as real-time transaction monitoring or compliance software are employed to detect suspicious activities Kroll, (2022).

While these mechanisms are standard across many organizations, their effectiveness often varies based on the department's expertise, the integration of technology, and the organization’s culture. The challenge lies in the need for continuous adaptation to keep up with evolving fraud tactics. physical security or manual audits, are becoming obsolete as fraudsters exploit digital vulnerabilities. Thus, organisations are gradually implementing technology enabled solutions like artificial intelligence, machine learning and big data analysis to improve fraud control systems Deloitte, (2021).

3.2 Operationalisation of theoretical constructs:

3.2.1 Occupational Fraud

Occupational fraud involves employees deceiving their employers for personal financial gain, leading to financial losses, reputational damage, and reduced employee morale. To mitigate this, organizations rely on anti-fraud controls, which can be preventive, detective, or corrective. Preventive controls aim to stop fraud before it happens, focusing on policies like robust hiring practices, employee education, and the establishment of an ethical workplace culture Alayli, (2022). These measures reduce the opportunities for fraud and increase the perceived risk of being caught. Detective controls are designed to identify fraud after it has occurred, relying on internal audits, data analysis, and whistleblower programs Davis, (2019). These mechanisms help organizations detect suspicious activities early, minimizing potential damage. Corrective controls, such as legal actions and recovery procedures, are implemented to mitigate the consequences of fraud once it is uncovered.

The COVID-19 pandemic forced organizations to adapt their anti-fraud controls due to shifts like remote work and digital transactions. Remote auditing, enhanced cybersecurity, and improved data analytics became essential in detecting fraud in this altered environment Efijemue et al., (2023). The evolving nature of fraud in the digital age underscores the importance of continuous fraud risk assessments. Ultimately, the effectiveness of anti-fraud controls depends on consistent implementation and commitment from leadership. Companies that focus on maintaining these controls, training employees, and using technology-driven solutions report fewer cases of occupational fraud Lang et al., (2023). However, challenges like evolving fraud tactics and resource limitations require organizations to remain vigilant and continuously update their controls. This ensures their defenses are robust and adaptable to new fraud risks.

3.2.2 Anti-fraud Controls

Anti-fraud controls are essential mechanisms to mitigate risks associated with financial fraud in organizations. Various studies emphasize the importance of robust internal control systems, employee training, and the use of technology in preventing and detecting fraudulent activities. According to Davis (2019), small retail businesses are particularly vulnerable to occupational fraud due to limited resources and less formalized control systems. Davis suggests that preventive measures such as segregation of duties, regular audits, and employee awareness programs are critical in safeguarding these businesses from fraud risks. Furthermore, employee background checks and encouraging a culture of transparency contribute significantly to fraud deterrence.

Internal controls play a pivotal role in fraud prevention across organizations of all sizes. Alayli (2022) highlights the impact of internal control practices in Lebanese small and medium enterprises (SMEs), where a lack of robust financial oversight often results in vulnerabilities to fraudulent activities. Alayli argues that implementing stricter internal controls, such as periodic reviews of financial statements, cash flow monitoring, and the establishment of whistleblowing channels, significantly reduces the likelihood of fraud occurrence. Properly designed controls not only detect fraud but also discourage employees from attempting fraudulent activities due to the high likelihood of being caught.

Additionally, cybersecurity measures have become increasingly critical in protecting financial institutions from fraud. Efijemue et al. (2023) emphasize the importance of cybersecurity strategies in safeguarding customer data and preventing financial fraud in the United States financial sectors. The study points out that integrating advanced technological tools, such as encryption, real-time transaction monitoring, and multi-factor authentication, can detect and prevent cyber fraud in its early stages. Overall, the combination of strong internal controls, employee vigilance, and technological defenses provides a comprehensive approach to preventing fraud in various organizational contexts.

3.2.3 Anti-fraud Controls in Preventing Occupational Fraud

Anti-fraud controls are crucial for preventing occupational fraud, which can have devastating financial and reputational consequences for organizations. Occupational fraud, typically involving employee misconduct, is mitigated by implementing robust internal controls, enhancing fraud detection mechanisms, and cultivating a culture of integrity. Kassem and Turksen (2021) emphasize that public auditors play a critical role in fraud detection by ensuring compliance with regulatory frameworks and conducting thorough reviews of financial practices. Auditors are key to identifying red flags and uncovering financial anomalies, thereby serving as a first line of defense against fraud.

The role of internal controls is pivotal in reducing occupational fraud. Abu Amuna and Abu Mouamer (2020) examine the impact of applying fraud detection and prevention instruments within the Ministry of Health in Gaza, revealing that strong internal controls, such as segregation of duties and routine audits, are essential in reducing occupational fraud. By separating financial duties among different employees, the risk of collusion and fraudulent behavior diminishes. Similarly, Kalovya (2023) explores the determinants of occupational fraud and stresses the importance of understanding both the offender’s motivations and the organization’s vulnerabilities to effectively mitigate fraud. An effective internal control system not only reduces opportunities for fraud but also acts as a deterrent to potential offenders.

Alayli (2022) further emphasizes the need for internal control practices in small and medium enterprises (SMEs) to reduce fraud risk. SMEs often lack formalized controls, making them susceptible to occupational fraud. Implementing practices such as regular financial audits and establishing whistleblower hotlines can strengthen an organization's defense against internal fraud. Additionally, technological advancements are reshaping anti-fraud strategies. Efijemue et al. (2023) highlight the importance of cybersecurity controls in safeguarding customer data and preventing occupational fraud in financial sectors. Advanced tools such as real-time monitoring, encryption, and multi-factor authentication help detect fraudulent activities before they escalate. Lang et al. (2023) also note the rising threat of cyber-enabled frauds, emphasizing that organizations must continuously adapt their controls to prevent emerging threats such as ransomware attacks. In conclusion, anti-fraud controls must encompass internal auditing, fraud detection systems, employee vigilance, and the integration of technology to prevent occupational fraud effectively. These measures, when combined, create a comprehensive fraud prevention framework that minimizes risks and enhances organizational resilience against fraud.

3.2.4 Post-pandemic Modifications

The COVID-19 pandemic significantly altered the global business landscape, resulting in changes in how fraud control mechanisms are applied. With businesses shifting to remote work environments and increasing reliance on digital systems, post-pandemic modifications to fraud control have become necessary to address evolving risks. Organizations have had to reassess their internal controls, strengthen cybersecurity, and adapt to new regulatory requirements to prevent fraud in this rapidly changing environment.

Levi and Smith (2022) explore how the pandemic triggered a surge in fraudulent activities, particularly within financial systems. As businesses moved online, cybercriminals exploited vulnerabilities in remote working setups, leading to an increase in both occupational and cyber-enabled fraud. Organizations, in response, have strengthened their fraud control systems by investing in advanced digital tools like real-time monitoring, fraud detection software, and encryption. These post-pandemic modifications are vital in preventing unauthorized access to financial systems and safeguarding sensitive data.

Internal controls, such as the segregation of duties and regular audits, have also been modified to suit the remote work environment. Kassem and Turksen (2021) highlight those public auditors, who traditionally relied on in-person reviews, now employ digital audits to detect fraud. This shift necessitates the implementation of digital audit trails, which enhance transparency and allow auditors to trace transactions more efficiently. However, the reliance on digital tools also requires organizations to continually train staff in fraud detection and cyber hygiene practices to reduce human errors that could lead to fraud.

Another significant post-pandemic modification is the enhanced role of cybersecurity in fraud prevention. Lang et al. (2023) examine how ransomware attacks surged during the pandemic and highlight the need for robust cybersecurity frameworks to prevent such attacks. Organizations now implement multi-factor authentication, encrypted communications, and enhanced data protection protocols to safeguard against cyber fraud. These modifications are critical, especially as more organizations conduct financial transactions online, increasing exposure to fraud risks. Moreover, the increased reliance on third-party vendors during the pandemic has prompted organizations to adopt more stringent due diligence and monitoring of vendors to ensure they do not introduce fraud vulnerabilities.

Kalovya (2023) points out that post-pandemic fraud controls have also shifted to focus on mitigating insider threats. With many employees working remotely, the lines between professional and personal activities have blurred, making it easier for occupational fraud to go unnoticed. To combat this, organizations are enhancing monitoring tools to detect unusual employee behaviors and financial anomalies. Automated fraud detection systems that use artificial intelligence (AI) and machine learning (ML) have become more popular in detecting patterns of fraud that may have previously gone unnoticed in a traditional office setup.

Furthermore, post-pandemic regulatory changes have also played a crucial role in shaping fraud control measures. Alayli (2022) mentions that regulatory bodies in various sectors have implemented stricter compliance requirements to address the increased risks of financial fraud in a remote working context. Organizations are now required to report suspicious activities more frequently and ensure that their fraud control systems are in line with updated regulations. These changes have prompted businesses to revisit their compliance strategies and integrate real-time reporting mechanisms to stay ahead of potential fraud. In conclusion, the post-pandemic landscape has prompted organizations to make several modifications to their fraud control strategies. Strengthening cybersecurity, enhancing internal controls for remote work, adopting AI-based fraud detection, and adhering to updated regulatory requirements are all essential for combating the rising threats of occupational and cyber-enabled fraud. By embracing these modifications, businesses can effectively safeguard their operations and reduce the risk of fraud in the new normal.

3.2.5 Effectiveness of Anti-fraud Controls

Stakeholders must place anti-fraud controls on organizational structures to avoid the occurrence, and detection of fraudulent activities. According to McCormack (2022), organizations in the financial sector are most at risk of occupational fraud by employees because of finances. It is because applications of MRS; Internal controls; Data analytics of the operation can lowest fraud risk down. In the same respect, Mwangi and Ndegwa (2020) realised that fraud risk management; involving board oversight, positive auditing, and staff support measures helped decrease the likelihood of fraud in Kenyan organisations. But more effort needs to be made as the perpetrators devise other ways of carrying out their scams. One of the major fraud prevention methods is enhancing an organization's ethical climate. Policies establish the standards of behavior required from personnel while conducting serves as information delivery on the policy and fraud plans. They also provide for reporting of suspicious behaviors to be addressed and for showing concern in the investigation of allegations (McCormack, 2022). Further improvements are to be done in the continuous process of developing integrity of all employees and leaders.

Maulidi and Ansell (2022) propose that controls ought to be restyled to combat current fraud methods such as cyber fraud among others. Program controls include separation of duties, no overlapping of employees' duties, conducting of their off-duty, and auditing of their terminals. Solutions based on technology introduce a certain level of automation in the following activities: verification of transactions, patterns' analysis, and integration of connections between data sources McCormack, (2022). The trade-off between the risk of loss and efficiency when updating controls to leverage innovations is reasonable. At a macro level of analysis, the roles of boards of directors include governance by conducting risk evaluations, audits, and review for accountability of anti-fraud programmes Mwangi & Ndegwa, (2020). Professional advice is used to improve policies while other reviews are used to assess the efficiency of the controls. For instance, general external audits focus on examining risky areas that are set down in accounting standards. Fraud risk management is, therefore, a continuous and progressive process supported from top to bottom. In brief, multiple layers used in integrity as well as in individual, process and governance aspects offer protection as against various frauds. However, complacency allows bypassing, therefore, the assessment is needed to be repeated frequently to contenders and the external environment. Authorities need to level the playing field with fraudsters by going digital, involving employees, directors, and committing to the subject of anti-fraud.

3.3 Research Purpose and Questions

As a result, the goal of the present research is to analyze the extent to which organizations are capable of preventing and detecting occupational frauds through the implementation of anti-fraud controls. Occupational fraud is defined as the unlawful or unauthorized utilization of one's position of work in order to chiefly enrich oneself, by missing or misapplying the organization's resources or tangible assets McCormack, (2022). Research done recently shows that occupational fraud is on the rise and many organizations across sectors are affected, opposite organizations for example, loses 5% of its annual income to fraud Mwangi & Ndegwa, (2020). However, fraud is not simply a problem concerning the direct monetary loss, but it can also lead to severe reputational losses and investors and stakeholders' distrust.

The research purpose of the study "Exploring the Impact of Anti-fraud Controls on Occupational Fraud" is to investigate the effectiveness of anti-fraud controls in mitigating the risk of occupational fraud within organizations. Occupational fraud poses a significant threat to organizations worldwide, leading to financial losses, damage to the organization's reputation, and negative impacts on employee well-being. The purpose of this research is to understand how anti-fraud controls can help organizations detect, deter, and prevent fraudulent activities, ultimately contributing to a more secure and ethical business environment.

The research aims to address the pressing need for effective measures to control fraud risks in organizations. With the complexity of modern business operations and the widespread adoption of Internet-based systems, occupational fraud has become more diverse and challenging to identify. As noted by the Association of Certified Fraud Examiners (ACFE), organizations globally lose approximately 5% of their annual revenue to fraud, highlighting the pervasive nature of this problem. Therefore, the primary purpose of this research is to contribute to the development of strategies and mechanisms that can assist organizations in effectively combating occupational fraud.

There has been a lot of emphasis on the use of various anti-fraud controls as a way through which organizations can deal with fraud risks. Anti-fraud controls are measures that are adopted to mitigate risks, discourage and identify fraud Carmichael & Lere, (2021). Such reviews comprise people’s confidential reporting to the company, internal auditing, management’s scrutiny of operations, and analysis of available data, respectively. However, there seems to be very little empirical research literature documenting the success of anti-fraud programs as such, let alone investigating their efficiency in diverse settings and industries. As for many other anti-fraud control elements, there is also not much data available on which exact mix of anti-fraud controls offers the best fraud fighting functionality. Furthermore, the research seeks to examine how the effectiveness of anti-fraud controls may be influenced by various factors, including the size of the organization, industry type, and the specific nature of issues faced by different departments. It aims to explore the nuanced relationship between organizational characteristics and the implementation of anti-fraud measures, recognizing that one-size-fits-all approaches may not be suitable for addressing the diverse needs of different organizations.

Research questions are:

- What are the key fraud prevention mechanisms currently employed by organizations, and how do these mechanisms vary across different departments, including HR, Accounting, Finance, Operations, IT, and other relevant departments?

- How have organisations modified their fraud prevention mechanisms in response to the global pandemic, and what specific adaptations have been made post-pandemic to enhance resilience against occupational fraud?

- To what extent have the modifications made to fraud prevention mechanisms post-pandemic been effective in preventing occupational fraud within various departments, and how does this effectiveness differ across departments?

- What commonalities and differences exist in the approaches to fraud prevention among organizations of different sizes and in different sectors, and how can these variations inform the development of targeted, department-specific strategies to enhance overall organizational resilience against occupational fraud?

Based on research questions, following hypothesis will be analysed during the study:

H01: There is no significant difference in the current utilization of fraud prevention mechanisms across various departments within organizations.

H11: There is a significant difference in the current utilization of fraud prevention mechanisms across various departments within organizations.

H02: There is no significant difference in the modifications made to fraud prevention mechanisms in response to the pandemic across organizations.

H12: There is a significant difference in the modifications made to fraud prevention mechanisms in response to the pandemic across organizations.

H03: There is no significant difference in the effectiveness of fraud prevention mechanisms before and after the pandemic across various departments.

H13: There is a significant difference in the effectiveness of fraud prevention mechanisms before and after the pandemic across various departments.

H04: There are no commonalities or differences in the fraud prevention approaches employed by organizations of varying sectors and sizes.

H14: There are commonalities and differences in the fraud prevention approaches employed by organizations of varying sectors and sizes.

3.4 Research Design:

Exploratory research design is applied when the problem to be investigated is unknown or unfathomable and there is little previous literature to consult. The goal is to get insights and be oriented more to the subject area for further research and potentially more scrutiny Allan, (2020). Explanatory research design is more advanced than descriptive research because the former seeks to establish cause-effect relationships. There is a great concern with observing the situation so that the researcher can describe causes or values attached to certain factors or features of a given phenomenon Al-Ababneh, (2020).

Grounded theory design is a purposeful approach by which theory is formed, not refuted or proven. It employs several levels of data collection and purification to develop the theory “grounded in data" Alharahsheh & Pius, (2020); Allan, (2020). Descriptive research design is meant to describe the; nature and attributes of the sample, the individual or the group and the incidence of any event or phenomenon. It deals with the identification of who, what, when, where and how questions Alharahsheh & Pius, (2020). The most appropriate approach to research design depends on the present level of knowledge about the research question and the individual research questions used. Explanatory and descriptive designs are relatively more formal than exploratory and grounded theory designs. All provide value in constructing information in a subject area of concentration.

Justification:

The use of a descriptive research design is justified in the current study for several reasons. First and foremost, a descriptive research design is well-suited for providing an accurate portrayal of the characteristics of a particular phenomenon. In this study, the aim is to provide a comprehensive overview of different types of research designs adopted in scientific studies, as well as to discuss the research approach and paradigm. A descriptive research design will enable the researchers to systematically gather data and accurately describe the various research designs and approaches that are prevalent in scientific studies. Furthermore, a descriptive research design will allow for the collection of both quantitative and qualitative data, which is essential for gaining a comprehensive understanding of the topic under investigation. By employing surveys, interviews, and observations, the researchers can gather rich and diverse data that will enable them to present a detailed and nuanced account of the different research designs and approaches. Additionally, a descriptive research design is conducive to generating new hypotheses and theories, which can further contribute to the existing body of knowledge in the field. Overall, the use of a descriptive research design is well-justified as it aligns with the objectives of the study and provides a robust method for systematically capturing and presenting the relevant information.

3.5 Population and Sampling

Sampling is also one of the research methods, it enables the choice of a limited number of persons so that generalization about a large number of people can be made. Non probability sampling techniques are; Random sampling, systematic sampling, stratified sampling, purposive, convenience and quota sampling. Probability sampling techniques fall under positivism research philosophies Al-Ababneh, (2020). These sampling techniques rely on the methodology of obtaining a sample by complete random selection from the various classes in the targeted population. While simple random sampling involves choosing of participants in total ignorance of where they come from, stratified random sampling organizes the total population into groups or ‘strata’ then picks participants randomly from each strata. In cluster sampling, sampling units are chosen at random in a group or cluster rather than the individual. Systematic sampling involves choosing participants in a regular manner rather than in a random manner, but still it is preferred. As a result of probability sampling, it is possible to make generalizations to the whole population and also quantify the extent of such generalizations in terms of confidence intervals as well as standard errors Allan, (2020).

Quota sampling is used with the goal of getting a sample with an across-the-board similarity to the overall population. Convenience sampling just uses the most convenient subjects and this involves inherent prejudices with it. In purposive sampling only the cases that the researcher feels are ‘‘information rich’’ with respect to the selected phenomenon are selected. Snowball sampling requires the participant currently involved to get other participants. Theoretical sampling the sample is modified from time to time to incorporate emerging concepts and important themes to build a theory as part of the process for an ongoing or initially identified theory Allan (2020). Non-probability sampling is ideal when the researcher wants to explore a phenomenon contextually, and qualitatively but cannot be used for generalization. Overall, the sampling technique has to suit the general research paradigms and research objectives. As dictated by the paradigmatic and methodological choice, researchers should choose a sample that is either a random sample or provides a lot of information on the targeted population. Random sampling process hence was followed for the study.

Justification:

Random sampling is a crucial method in research methodology, particularly in studies aiming to achieve generalizability and minimize bias. The justification for using random sampling in this study on the impact of anti-fraud controls on occupational fraud is rooted in its ability to provide an unbiased representation of the population under investigation. By employing random sampling, every individual or unit within the population has an equal chance of being selected for the study, thus reducing the potential for selection bias and allowing for the generalization of findings to the broader population.

In the context of this study, the use of random sampling ensures that all relevant stakeholders and elements within organizations, regardless of their specific roles or characteristics, have an equal opportunity to be included in the sample. This is particularly important when investigating the impact of anti-fraud controls, as it allows for a comprehensive and representative assessment of the effectiveness of these measures across different organizational functions, sizes, and industries.

Furthermore, random sampling enhances the statistical validity of the study by allowing for the application of inferential statistics to draw conclusions about the population based on the sample data. This is essential for making evidence-based recommendations and insights that can be applied to diverse organizational settings confronting occupational fraud. Moreover, the use of random sampling aligns with the ethical considerations of fairness and inclusivity, as it ensures that all relevant stakeholders have an equal chance of being included in the study, thereby avoiding potential biases in the selection process. In summary, the justification for using random sampling in this study lies in its ability to provide a representative and unbiased sample, enhance statistical validity, and align with ethical considerations of fairness and inclusivity. The use of random sampling in this research methodology is essential for obtaining reliable and generalizable insights into the objectives.

The research population of the study includes employees responsible for fraud prevention mechanisms, including managers, and senior officials across various departments within organizations. The section will also describe the sampling technique used in this study.

3.6 Participant Selection

The participant selection process in a study is a crucial aspect that directly impacts the quality and reliability of the research findings. The process of selecting participants involves identifying and recruiting individuals or groups who possess the characteristics and experiences relevant to the research objectives. In the context of exploring the impact of anti-fraud controls on occupational fraud, the participant selection process is particularly important in ensuring that the study captures diverse perspectives and experiences related to fraud prevention and detection within organizations.

One of the key considerations in the participant selection process is defining the target population. In this study, the target population may include employees at various levels within organizations, such as accounting and finance professionals, human resources personnel, and senior management involved in anti-fraud measures. Additionally, the selection process should take into account the specific criteria for inclusion, such as years of experience in the organization, exposure to anti-fraud controls, and involvement in fraud detection or prevention activities.

The sampling technique employed in participant selection also plays a significant role. Depending on the research design and objectives, the study may utilize techniques such as random sampling, stratified sampling, or purposive sampling. For instance, random sampling can help ensure that each member of the target population has an equal chance of being selected, while purposive sampling allows for the deliberate selection of participants based on their expertise and relevance to the research focus.

Furthermore, ethical considerations should guide the participant selection process. It is essential to obtain informed consent from the participants, ensuring that they understand the purpose of the study, their role, and the potential impact of their participation. Confidentiality and anonymity should be maintained to protect the privacy of the participants, especially when discussing sensitive topics such as past experiences with fraud or anti-fraud measures.

Moreover, the participant selection process should aim to achieve diversity and representation. Efforts should be made to include participants from various organizational sizes, industries, and geographic locations to capture a comprehensive understanding of the impact of anti-fraud controls on occupational fraud across different contexts.

In summary, the participant selection process in this study was systematic, ethical, and inclusive, aiming to gather diverse perspectives and experiences that contribute to a comprehensive exploration of the impact of anti-fraud controls on occupational fraud within organizations.

3.7 Instrumentation

A survey is a research method used to collect data from a specific group of people to gain insights into their thoughts, opinions, and behaviors. Surveys can be conducted through various means such as online questionnaires, telephone interviews, face-to-face interviews, or paper-based questionnaires. Surveys are a popular research instrument due to their versatility, cost-effectiveness, and ability to gather a large amount of data from a diverse population.

One of the key justifications for using surveys as a research instrument is their ability to gather data from a large and diverse sample of the population. Surveys allow researchers to reach out to a wide range of individuals, regardless of their geographical location, making it possible to collect a broad spectrum of opinions and experiences. This inclusivity is particularly beneficial when studying a topic that is relevant to a diverse population, as it ensures that a wide range of perspectives are considered in the research.

Furthermore, surveys provide a structured approach to data collection, allowing for standardized data gathering and analysis. This consistency is crucial for ensuring the reliability and validity of the research findings. By using well-designed survey questions and response options, researchers can minimize bias and ensure that the data collected accurately reflects the participants' viewpoints. Additionally, surveys allow for the collection of both qualitative and quantitative data, providing researchers with a comprehensive understanding of the topic under investigation.

Surveys also offer a cost-effective and efficient means of data collection. Compared to other research methods such as interviews or focus groups, surveys can reach a larger audience at a lower cost. With the advancement of online survey platforms, researchers can easily design, distribute, and collect responses from participants, saving both time and resources. This accessibility makes surveys a practical choice for researchers working within limited budgets or time constraints. In conclusion, surveys serve as a valuable research instrument due to their ability to gather diverse data from a large sample, provide standardized data collection, and offer a cost-effective means of data gathering. By utilizing surveys in research, researchers can gain comprehensive insights into the thoughts, opinions, and behaviors of the target population, contributing to a more robust and well-rounded study.

3.8 Data Collection Method:

Data collection plays a critical role in research as it provides the foundation for analyzing and drawing conclusions about the research questions or hypotheses. In any study, collecting accurate, reliable, and relevant data is essential to validate findings and offer insightful contributions to the field. As Allan, Rangarajan, and Shields (2021) point out, working hypotheses in deductive exploratory research are guided by the collection of data, which is integral to examining causal relationships and testing theoretical frameworks. The process of gathering information ensures that the research maintains objectivity and transparency, providing a clear picture of the phenomena being studied.

In terms of research methodology, the significance of data collection cannot be overstated. Data is the cornerstone that drives analysis, interpretation, and the formulation of meaningful conclusions. Researchers must adopt suitable data collection methods based on the nature of their study, which will impact the validity, reliability, and generalizability of the results. The selection of methods hinges on the research paradigm—whether qualitative, quantitative, or mixed-each offering different strengths in exploring complex research questions.

There are various methods of data collection utilized by researchers, with the choice largely depending on the research design, objectives, and questions. Two broad categories of data collection methods are primary data and secondary data.

Primary Data Collection

Primary data collection refers to the process of gathering first-hand information directly from sources, which allows researchers to gather data that is specific and relevant to their study. This approach is particularly valuable in studies that require detailed and original insights into human behavior, opinions, or real-world phenomena.

Surveys and Questionnaires: These are structured tools used to collect data from large groups of people. Surveys are widely used in quantitative research, allowing researchers to collect standardized responses from participants, which can be statistically analyzed. Surveys are especially effective in exploring attitudes, opinions, and demographic information Bianchi, (2021).

Interviews: A common method in qualitative research, interviews allow researchers to gather in-depth information from participants through open-ended questions. This method provides rich, detailed data that can help uncover underlying motives and perceptions that may not be captured through quantitative methods Khatri, (2020).

Observations: Observation is often employed in studies that focus on behaviors or actions in natural settings. This method involves researchers immersing themselves in the environment they are studying, either as passive observers or active participants, to collect direct data on specific behaviors or events.

Focus Groups: Focus groups bring together a small group of participants to discuss a particular topic, allowing researchers to observe interactions and gather insights into group dynamics and collective perspectives. This method is especially useful for exploratory studies that aim to understand broader social and cultural patterns Kandel, (2020).

Secondary Data Collection

Secondary data refers to data that has already been collected and published by others. It includes statistics, reports, or research findings from government bodies, academic institutions, or industry reports. While secondary data is useful for comparative analysis or validating findings, it lacks the specificity and context that primary data offers for original research.

Document Analysis: Researchers may review existing documents, including government publications, policy papers, historical records, or previous research studies, to gather insights or baseline data for their own investigations.

Databases and Repositories: Online databases provide a wealth of secondary data, ranging from demographic statistics to market research reports. Researchers often rely on secondary data when time or resources for primary data collection are limited.

Justification

In this study, the use of primary data collection is particularly justified due to the need for specific, real-time, and context-driven data that secondary sources may not provide. Allan, Rangarajan, and Shields (2021) highlight the importance of first-hand data in exploratory research, especially when developing and testing working hypotheses. Primary data allows the researcher to tailor questions or observations directly to the subject matter, ensuring that the data collected is relevant and addresses the research objectives. Moreover, primary data collection provides flexibility and control over the research process. Researchers can modify questions, delve deeper into areas of interest during interviews, or observe specific behaviors in real-time. In contrast, secondary data may not align with the precise focus of the study, limiting its applicability and depth. For example, in studying fraud control mechanisms in post-pandemic environments, researchers might conduct interviews with industry professionals or financial experts to understand how companies have adapted their strategies. This real-time data would provide fresh insights that secondary sources might not capture.

Furthermore, primary data is crucial for the analysis of emerging trends or phenomena where existing literature is scarce. As Kirongo and Odoyo (2020) point out, in fields like information technology, where rapid changes occur, secondary data may quickly become outdated. By collecting primary data, researchers ensure that the information is current and reflects contemporary challenges and strategies. In qualitative research, such as exploratory studies that aim to uncover new patterns or relationships, primary data is indispensable. It allows for deep exploration of participants' experiences, thoughts, and opinions, which are often necessary for developing grounded theories or insights. According to Kandel (2020), qualitative methods such as interviews and focus groups provide rich data that quantitative methods or secondary sources may not capture, further justifying their use in research contexts requiring a nuanced understanding of human behavior. In conclusion, while secondary data has its uses, the collection and analysis of primary data in this study are critical for ensuring specificity, relevance, and control over the research process. Primary data enables the researcher to explore real-time issues, gather firsthand insights, and tailor data collection methods to the unique demands of the research questions. By employing a combination of surveys, interviews, or observations, researchers can gather original, detailed data that directly addresses the core objectives of the study.

3.9 Data Analysis and Interpretation

Secondary data analysis therefore refers to the process where data, which was collected by someone else for another purpose other than answering the current research questions is used. Further it enables researchers to engage in research in a cost and time efficient manner Kandel, (2020). In light of the research philosophy that shall have been adopted, there are diverse approaches and techniques for analysing such data. However, in the study, Quantitative analysis is used, which includes hypothesis testing, regression, analysis of variance, factor analysis and so on Interpretivists use qualitative data analysis techniques such as thematic analysis content analysis and so on in order to gain their conceptual understandings and insights of human experiences and behaviours from secondary narratives, images, audio-visual data etc. Khatri, (2020).

The adoption of statistical methods for data analysis is critical in research, particularly when exploring the impact of anti-fraud controls on occupational fraud. Quantitative data analysis provides an objective and empirical means of validating hypotheses and assessing relationships between variables. Statistical methods help in summarizing data, testing relationships, identifying patterns, and making predictions based on empirical evidence. In this study, the use of statistical methods via IBM SPSS (Statistical Package for the Social Sciences) is justified for its robust capabilities in handling complex quantitative data efficiently.

According to Muhaise et al. (2020), the choice of a statistical tool is crucial in ensuring that research outcomes are accurate and reliable, especially for postgraduate students grappling with complex datasets. ***IBM SPSS,*** a leading software for quantitative analysis, offers a wide range of tools to conduct descriptive and inferential statistical tests, including regression analysis and ANOVA test. These tools are necessary to examine the relationships between anti-fraud controls and occupational fraud in this study. The decision to adopt statistical methods is also guided by the deductive research approach, where hypotheses are tested based on established theories. Okoli (2023) highlights the importance of deductive theorizing in research that involves testing pre-determined hypotheses. In this context, statistical analysis is indispensable for validating these hypotheses by providing numerical evidence that supports or refutes them. For example, by applying regression analysis in SPSS, the study can assess how certain anti-fraud measures (e.g., internal audits, fraud detection systems) directly impact the occurrence of occupational fraud.

Moreover, the use of IBM SPSS ensures precision in handling large datasets, minimizing the risk of human error in manual calculations. Nur (2020) emphasizes the role of software tools like SPSS in streamlining data analysis, as they offer an intuitive platform for users to perform sophisticated statistical tests without extensive manual computation. In the context of this study, SPSS enables the researcher to quickly generate results, run tests, and visualize data through graphs and charts, aiding in better interpretation and presentation of findings. Saunders et al. (2023) underscore the importance of choosing analytical tools that align with the research objectives and data type. In this study, statistical methods such as correlation tests, which measure the strength of the relationship between anti-fraud controls and fraud outcomes, will be essential. These methods allow for a rigorous examination of the effectiveness of various controls in reducing fraud occurrences.

3.10 Research Design Limitations:

When considering research design limitations, it's essential to acknowledge that no research design is without its constraints. One common limitation is the potential for bias. Research designs may inadvertently introduce biases due to factors such as sample selection, measurement tools, or researcher influence. For example, in a survey-based research design, the wording of the questions or the order in which they are presented can influence participants' responses, leading to biased results. Another limitation is the generalizability of findings. Many research designs, especially those based on specific samples or contexts, may not allow for broad generalizations to be made. For instance, findings from a study conducted in a specific geographical location or cultural setting may not be applicable to other regions or cultures.

Additionally, research design limitations can stem from practical constraints such as time, budget, and access to resources. These constraints may impact the scope and depth of the study, potentially limiting the extent to which the research questions can be adequately addressed. Furthermore, ethical considerations and human subject constraints can pose limitations on the research design. For example, certain research questions may involve sensitive topics or populations, leading to constraints in data collection and analysis due to ethical and privacy concerns. Lastly, the dynamic nature of research topics and environments can also present limitations. Research designs are often static, while the real world is constantly evolving. This misalignment can make it challenging for research designs to capture the full complexity and nuances of the phenomena under study. Overall, acknowledging and addressing these limitations is crucial for ensuring the transparency and validity of research findings.

3.11 Ethical Considerations:

The ethical considerations of this study include ensuring informed consent from all participants, guaranteeing their right to withdraw at any time without penalty. Confidentiality and anonymity must be maintained to protect participants' identities and sensitive information. Data collection procedures should be transparent, and participants should be made aware of the study's purpose and potential impacts. Additionally, the study will adhere to ethical guidelines established by relevant institutional review boards to prevent any harm to participants. Researchers must also be honest and transparent in reporting findings, avoiding any manipulation or misrepresentation of data.

3.12 Conclusion:

Chapter 3 delves into the research methodology employed in the study, emphasizing the significance of research instruments in achieving the research objectives. It discusses the selection and justification of research instruments, such as surveys, interviews, and observations, to gather data effectively. The chapter also addresses the importance of aligning the instruments with the research questions, ensuring their reliability and validity, and adhering to ethical considerations. Overall, the research methodology chapter serves as a roadmap for conducting the study, enhancing the credibility and trustworthiness of the research through the careful selection and utilization of research instruments.

CHAPTER IV: RESULTS

4.1 Demographics of Respondents

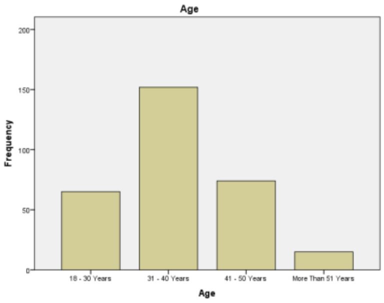
Table 4.1: Age Distribution

- 49.7% of the respondents are of 41-50 years Category

Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18 - 30 Years	65	21.2	21.2	21.2
	31 - 40 Years	152	49.7	49.7	70.9
	41 - 50 Years	74	24.2	24.2	95.1
	More Than 51 Years	15	4.9	4.9	100.0
	Total	306	100.0	100.0	

Figure 4.1: Age Distribution



The distribution into age groups is an indication of the varied composition of the workforce that is insinuated within the study sample. Most of them, 49.7% fall between the 31-40 years age bracket. It is a mid-career demographic likely to bear important responsibilities in an organization. They provide appropriate insights into mechanisms for fraud prevention since at this level they must have some practical experience in dealing with such challenges.

The second largest is the 41-50 years category, comprising 24.2% of the respondents. This age bracket often includes senior-level professionals or managers with lifelong experience who can add strategic perspectives in the implementation and overseeing of anti-fraud controls. These two groups together take nearly three-quarters of the participants, meaning that a well-represented professional spectrum exists.

18- to 30-year-olds consist of 21.2% of the respondents and are the young professionals who are in an entry-level or junior position in the occupation. This, therefore, will make their responses of utmost value while trying to get an understanding of the effectiveness of fraud mechanisms from the grassroots perspective. Bringing it full circle, 4.9% of the respondents were over 51 years of age and can bring wisdom and institutionalized knowledge to fraud prevention.

The Occupational Fraud 2024 report shows that the highest median losses were by perpetrators aged 31–50 years, reflecting their positions of authority or trust. The losses caused by employees who were less than 30 years old were low, often confined to simpler schemes like asset misappropriation due to restricted access. Older fraudsters are more likely to have much experience and knowledge of the organization and, thus, be involved in complex frauds such as corruption or financial statement fraud. Diversity in the various age groups ensures that a holistic understanding is gained of how different experience levels perceive and interact with the organizational fraud prevention measures, thereby enriching the findings of this study.

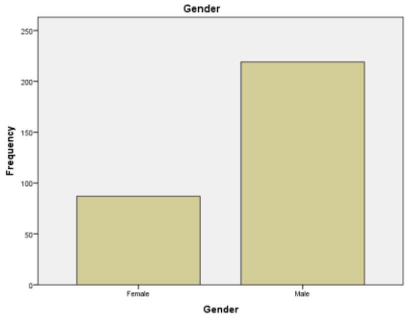
Table 4.2: Gender Representation

- 71.6% of the respondents are Female.

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	87	28.4	28.4	28.4
	Male	219	71.6	71.6	100.0
	Total	306	100.0	100.0	

Figure 4.2: Gender Representation



The gender distribution of the study sample indicates that the male respondents constitute the majority, with 71.6% of the total. This constituency shows that there was a male dominance in the organization under study. Male respondents likely hold a diverse range of positions throughout the departments, thereby giving a wide perspective of the implementation and effectiveness of fraud prevention mechanisms.

Females constitute 28.4% of the total, a smaller but effective presence in the workforce. This is a useful demographic insight into the gender perspective on occupational fraud and the possibility of variant perspectives being brought into the framing of anti-fraud strategies. With an increasing emphasis on professional settings being more gender-inclusive and diverse, this representation provides an interesting look at how organizations address fraud prevention in an evolving workplace.

The gender composition also opens avenues for probing whether differences in roles, responsibilities, or departmental concentrations influence fraud risk perception and the efficacy of prevention mechanisms. This dynamic, if understood, might also assist the organization in framing the training and communication strategies to better engage different groups.

The participation of these genders in this study is indicative of the importance of inclusivity in constructing a comprehensive and effective fraud prevention framework that would resonate across all employee demographics.

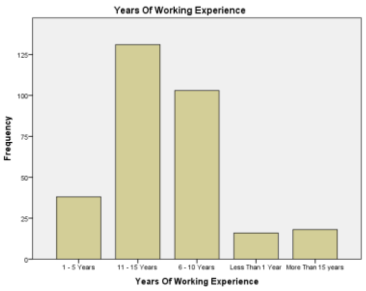
Table 4.3: Work Experience

- 42.8% of the respondents are 11-15 years of experience Category.

Years Of Working Experience

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 - 5 Years	38	12.4	12.4	12.4
	11 - 15 Years	131	42.8	42.8	55.2
	6 - 10 Years	103	33.7	33.7	88.9
	Less Than 1 Year	16	5.2	5.2	94.1
	More Than 15 years	18	5.9	5.9	100.0
	Total	306	100.0	100.0	

Figure 4.3: Work Experience



The distribution of respondents' work experience is a good mix of professional tenures, thereby enriching the research with insights from different career stages. The largest proportion of the respondents, 42.8%, falls within the category of 11-15 years of work experience. This mid-career demographic may be expected to include employees in key operational or managerial positions and thus informed on critical issues about pragmatic implementation and supervision of fraud prevention mechanisms.

The second-largest group, with 33.7% of the respondents, has 6-10 years of experience. These professionals in early management or specialized roles provide valuable input on how the anti-fraud strategies are implemented and crucially, how well they work in reality. Their experience bridges the gap between the entry-level tasks and the more strategic responsibilities, thus often providing a very balanced view of organizational practices.

Respondents with 1-5 years of experience constitute 12.4% of the total sample and are considered early-career professionals, mainly involved in operational roles. In this context, their responses indicate how well fraud prevention mechanisms are communicated and implemented at the grassroots level. Another 5.9% of the respondents have more than 15 years of experience, bringing seasoned expertise and, in most cases, institutional knowledge into the discussions.

This distribution is important because it will contribute to a wider understanding of how fraud prevention mechanisms are perceived and implemented at different stages of career progression, therefore providing nuanced insights into organizational practices.

Departmental Representation

Table 4.4: Total Employees in your department?

- 41.5% of the respondents have 101 and more employees.

Department

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	101 and more	127	41.5	41.5	41.5
	26-50	36	11.8	11.8	53.3
	1-10	37	12.1	12.1	65.4
	11-25	33	10.8	10.8	76.1
	51-100	73	23.9	23.9	100
	Total	306	100.0	100.0	

Figure 4.4: Total Employees in your department?

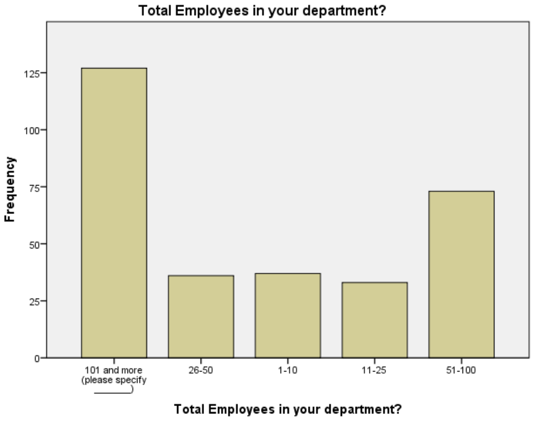


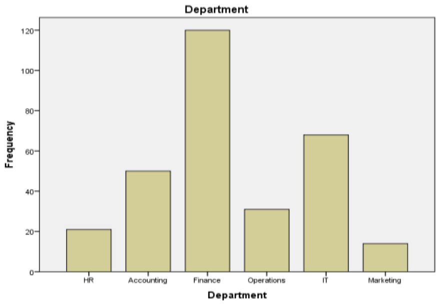
Table 4.5: department

- 39.5% of the respondents belong to the Finance Department.

Department

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	HR	21	6.9	6.9	6.9
	Accounting	50	16.3	16.4	23.4
	Finance	120	39.2	39.5	62.8
	Operations	31	10.1	10.2	73.0
	IT	68	22.2	22.4	95.4
	Marketing	14	4.6	4.6	100.0
	Total	304	99.3	100.0	
Missing	System	2	.7		
Total		306	100.0		

Figure 4.5: department



This shows a reasonably good representation of organizational functions, with very useful input from departments most directly involved in the prevention and management of fraud. The Finance department is the largest segment, with 39.5% of respondents. This is expected since finance professionals are at the heart of tracking and protecting financial transactions, and thus their views on anti-fraud measures are crucial. As per the occupational fraud report 2024 it is noted that financial statement frauds are the least common but more costly.

The IT departments are represented by 22.4% of the respondents to this survey, as the fraud world increasingly depends on technology both in committing and detecting fraud. In fact, IT professionals are needed for valuable insights into cybersecurity measures, technological advancement, and system vulnerabilities that could affect fraud risk exposure.

The Accounting department, which consists of 16.4% of respondents, carries out its role under the purview of audits and reporting to ensure the integrity of financial matters. Operations comprise 10.2%, contributing its representational inputs in terms of procedural compliance and operational risks. In contrast, smaller contributions come from HR at 6.9% and Marketing at 4.6%, highlighting how fraud prevention is organized through cross-functional involvement. The role of HR underpins major importance in training and policy-based policy in fostering an ethical workplace culture, while marketing shows the care for customer interaction and protection of brand reputation. These will ensure that the understanding of fraud prevention strategies for various departments remains balanced. The cross-departmental insights underpin the fleeting nature of anti-fraud mechanisms and collaboration in putting them into place within different contexts.

Findings from Research Questions

4.2 Research Question 1

What are the key fraud prevention mechanisms currently employed by organizations, and how do these mechanisms vary across different departments, including HR, Accounting, Finance, Operations, IT, and other relevant departments?

4.2.1 Usage Across Departments

These findings denote that there are significant differences in the fraud prevention mechanisms employed by organizational departments, clearly supported by the analysis performed using ANOVA. Each department has different roles and responsibilities within the organization, which influences how it employs or views fraud prevention mechanisms; hence, the need for tailor-made strategies.

Hence, the Finance department also comes across as a very important center for fraud prevention activities, with 39.5% of the respondents. Directly overseeing all the transactions and budgeting for compliance, finance professionals can only trust fraud detection tools, internal audits, and monitoring systems to lessen risks in this case. Additionally, the department will play a very important role in aligning fraud prevention efforts with regulatory requirements and industry standards concerning the maintenance of financial integrity.

IT is equally important because it is the backbone in combating fraud risks implored by technology. IT professionals run fraud detection systems quite frequently, including AI and machine learning tools, to help uncover patterns indicative of fraudulent activities. They also focus on cybersecurity in protecting sensitive information: data encryption, multi-factor authentication, and monitoring systems to avoid information breaches.

Accounting focuses on internal controls for robustness, financial reporting for accuracy of records, and identification of discrepancies indicative of fraud. This department often stresses compliance with policies and procedures and may coordinate with Finance to strengthen overall fraud prevention efforts.

The Operations department contributes 10.2% by ensuring that day-to-day processes conform to the set guidelines and, hence, minimize the risk of procedural or operational fraud.

Their engagement in the application of fraud prevention mechanisms often focuses on observing workflows for inefficiencies that may be open to exploitation.

The supporting role of the human resource department, which accounts for 6.9%, is done through fraud prevention training programs, embedding a culture of ethics and accountability. HR's emphasis on employee awareness and behavior facilitates tackling fraud risks linked to collusion, rationalization, or internal policy violations.

The following includes fraud prevention mechanisms, which the Marketing department appeals to in securing the customer interaction and protects brand integrity at 4.6%. Monitoring for possible fraud in digital campaigns and payment platforms is involved herein, sometimes even in e-commerce sites.

As confirmed by the ANOVA results, there are very significant differences concerning the level of utilization, frequency of updates, and degree of collaboration among departments. This is an indication of the need for a department-by-department fraud prevention approach in order to take account of the unique needs and challenges of each department, having in mind genuinely effective and comprehensive anti-fraud strategies that would focus on general organizational resilience against occupational fraud.

4.2.2 Sectoral Differences

The results from regression analysis underline certain marked sectoral variations in the usage of fraud prevention mechanisms by organizations, which in turn underlines the importance of tailored approaches with regard to unique challenges in each industry. It underlines the impact of industry-specific risks, regulatory requirements, and related operational habits in shaping fraud prevention strategies within organizations. Also as per the Occupational Fraud Report 2024 the industries with the greatest median losses were mining (USD 550,000), wholesale trade (USD 361,000), and manufacturing (USD 267,000).

Financial Sector High-volume transaction with strident regulatory requirements, the financial sector deploys some of the advanced fraud prevention mechanisms. Using continuous AI and ML algorithms, organizations in this sector keep track of all real-time transactions to recognize anomalies and patterns which suggest fraud.

Regulatory compliance, like AML and SOX requirements, is also an important part of such mechanisms. Multi-layered defense includes data encryption and automated reporting systems to further enhance fraud detection and prevention efforts.

IT Sector

Cybersecurity is one of the most critical sectors in the IT industry, which has lately faced a number of large-scale data breaches and system exploits. Network security measures, such as firewalls, multi-factor authentication, and encryption protocols, are taken as headline strategies in fraud prevention within this sector. IT departments can use various advanced analytics and monitoring tools to identify and spot several weak points in real time, which again points out the technological integration happening within this sector.

Retail Sector

The retail industry is one of the most vulnerable when it comes to payment fraud, return fraud, and inventory theft. Companies in this vertical integrate fraud detection systems with the POS system and online payment systems to monitor inconsistent transactions. Increasing adoption of e-commerce has driven tokenization and encryption technologies to preserve customer data. Employees at retailers also conduct training related to the prevention of internal fraud, especially in handling cash and inventory.

Healthcare Sector

The industry-specific fraudulent exposures dealt with in the industry include insurance fraud, billing fraud, and misappropriation of assets, among others. It utilizes specific fraud prevention mechanisms, forensic accounting, and compliance audits, together with training programs in ethical practices for employees. This would also mean that within the sector, emphasis is being given to EHR systems which are highly secure, minimizing chances of data breach incidents.

Manufacturing Industry Manufacturing companies also implement measures to prevent fraud targeted at procurement fraud and mismanagement of inventory. Strategies involve vendor audits, supply chain monitoring, and separation of duties. These days, tracking technologies like RFID and blockchain are increasingly used to ensure that the supply chain is transparent and accountable. Cross-Sectoral Insights Regression analysis further shows that mechanisms that avoid fraud are considerably different across industries, based on operational risks and priorities. This designs a tailor-made approach to make the strategies relevant and appropriate, hence indicating that adaptations concerning the industries are of utmost importance in fraud combat.

4.2.3 Organizational Size

The size of an organization is a key factor in drawing methodology in devising and implementing fraud prevention mechanisms; large and small organizations have devised ways of suiting challenges and resource capacities to the peculiar natures of such organizations. Confirmations through regression analysis support such views that differences in size shape the perceptions of risks and allocations for resources to fight fraud. The Occupational Fraud 2024 report shows very clearly that the size in organization makes a difference in fraudulent cases. Smaller organizations suffer disproportionately high financial damage relative to their size, with median losses of $141,000, whereas larger organizations showed higher absolute losses, with a median loss of $200,000 due to big complexities and huge operations. However, they quite often use advanced technologies such as AI, robust internal controls, and "three lines of defense" models to deter and detect fraud.

Large organizations

Large organizations feature complex organizational systems and a lot of resources. Because of these reasons, they can use quite sophisticated strategies in fraud prevention. Some advanced technologies deployed in such organizations for the detection of fraud in real-time are AI, ML, and blockchain. AI-powered systems allow large firms to monitor high-volume transactions, find anomalies, and automate fraud detections in near real-time, hence greatly reducing response times.

Larger organizations have a compliance department to oversee fraud prevention activity of a risk management team. Some common best practices for large organizations include enterprise-wide risk assessments, internal audits, and whistleblower hotlines. Large firms are very often subject to a number of regulatory requirements that require stringent internal controls, such as SOX for finance and/or HIPAA for healthcare. The typical model used in large organizations for fraud prevention is "three lines of defense": first, operational management; second, risk management; and third, internal and external audits.

Small-scale Organizations

Small organizations have various challenges. The general characteristics involve fewer resources, fewer personnel, and rigidity in procedures. Without the sophisticated technologies available to other companies, at times they substitute this with more effective, focused, and inexpensive solutions. Small businesses still rely on extending the manual controls such as job separation, periodic monitoring of cash flow, and inventories for preventing theft or fraud. A very important approach in which the employee workforce can become a first line of defense involves training them for ethical behavior and fraud awareness.

The small organization can use collaborations and outsiders' expertise also. If the fraud risk goes higher, forensic accountants could be hired or resort to audits of third parties. For example, in retail or the hospitality context, small business owners can utilize some low-cost fraud detection tool that is integrated into a Point-of-Sale system that continuously monitors transactions to detect abnormalities.

Commonalities Across Sizes

In every organization, whether big or small, the need to create a workplace environment intolerant of fraud is emphasized. The programs for employee training and reporting procedures are the same for all. Whistleblower hotlines and mechanisms for anonymous reporting were shared across economies in recognition of the common objective of ensuring vigilance on the part of employees.

These best practices include embedding state-of-the-art technologies, embracing risk-based auditing, and maintaining collaboration across departments. Smaller organizations should focus on stringent internal controls, holding staff accountable, and leveraging third-party expertise to help minimize fraud-related risk. Ultimately, the extent of implementation may vary, but large and small organizations alike can benefit greatly from a fraud prevention strategy tailored to their needs and limitations.

4.3 Research Question 2

How have organizations modified their fraud prevention mechanisms in response to the global pandemic, and what specific adaptations have been made post-pandemic to enhance resilience against occupational fraud?

4.3.1 Pre-Pandemic Measures

Before the outbreak of the COVID-19 pandemic, organizations used different established fraud prevention mechanisms aimed at forestalling occupational fraud. In this respect, the basic enabling mechanism has traditionally been constitutive of strong internal control, frequent audits, and employee awareness programs that form the backbone of fraud prevention policies or programs. The Occupational Fraud 2024 report indicates some interesting trends in fraud loss and detection. Median fraud losses increased by 24% during the pandemic, reflecting increased vulnerabilities due to remote work and operational changes.

Internal controls prevented or detected the fraud. Typical activities that were employed included separation of duties, approval of financial activities, and documentation in support of the same goal-to minimize fraud events. The organization also often would conduct regular internal and external audits to assess financial activities, identify weaknesses, and recommend changes. While effective, these controls tended to be reactive and could not keep pace with emerging methods of committing fraud.

Other key pre-pandemic measures included fraud risk management policies. These involved periodic risk assessments in search of highly vulnerable areas within an organization, making fraud response plans, and putting in place a program. Anonymous reporting systems allowed employees to report suspicious activity without fear of retaliation; such reporting systems fostered a culture of accountability and vigilance.

It also increasingly involved data monitoring and analytics, especially in areas like finance and retail, where hundreds of thousands of transactions would occur in a very short period. Tools like data mining and pattern recognition helped organizations flag irregularities in real time. However, these systems were less sophisticated compared to the later-on AI-powered solutions.

Pre-pandemic measures included employee training and compliance programs. Companies invested in fortifying employees as the first line of defense through educating them on fraud risk, ethical behavior, and regulatory compliance. While these measures proved effective, they were most times bound by static processes unable to move at the increasing rate within which fraud tactics change, even more so with emerging technologies during the pandemic.

4.3.2 Post-Pandemic Adjustments

The COVID-19 pandemic compelled a sea change in organizations regarding fraud prevention mechanisms to meet the new risks presented by teleworking, operational disruption, and the increasing reliance on technology. These changes were necessary so that adaptation could be made to the newly emerging vulnerabilities created by the rapid changes in the job environment. How the process of fraud prevention measures adapted to the remote environments of work was, in fact, a huge leap. Traditional internal controls faced challenges related to the segregation of duties as employees donned multiple hats. In response, the organizations enhanced their digital security measures through methodologies such as multi-factor authentication, secure remote access, and virtual monitoring systems that would maintain integrity in distributed work environments.

The second most important adjustment dealt with deeper reliance on advanced technology. Most organizations relied on AI-driven fraud detection systems, machine learning algorithms, and data analytics to find out suspicious activities in real-time. These were quite effective in addressing the growing complication of fraud across the finance and IT sectors. Organizations also had to upgrade their employee training programs to match the evolution of conditions leading to the fraud risk. Employees were virtually taken through a session aimed at creating awareness about the cyber fraud, vulnerabilities of working from home, and fraud reporting procedures that have changed. This increased the ability of employees to recognize and report fraudulent activities.

Another emphasis was on the increased collaboration between its different departments. Likewise, other functional departments like Finance, IT, and HR began to collaborate to harmonize the fraud prevention mechanism with new operational realities. This includes regular risk assessments, technology upgrades, and cross-functional fraud detection strategies. These post-pandemic adaptations underline the ability to adapt and collaborate in effective fraud prevention structures that make an entity resilient to fraud risks in the post-pandemic era.

4.3.3 Increased Awareness Post-Pandemic

On one side, a statistical analysis underlines an extraordinary increase post-pandemic in Employee Confidence and Engagement with their fraud prevention. This 'shift towards remote work came with increased demands for improved communique, training, related to technology, and raising awareness against fraudulent risks.' These means have forged the potential way leading to a new culture in every organizational platform: proactive through awareness, and accountability (ACFE, 2022).

Improved employee training and awareness One of the most critical changes in the post-pandemic era has been remodeling employee training programs. Organizations introduce targeted, virtual training sessions on emerging fraud risks, such as cybersecurity threats and vulnerabilities associated with remote work environments. This increased emphasis has significantly improved employees' ability to recognize and report fraudulent activities, as indicated by a notable rise in confidence levels. Studies have shown that well-trained employees are more likely to act as the first line of defense against fraud.

Statistically Significant Increase in Engagement

ANOVA from this study presents the positive and statistical significance of the rise of employee engagement in fraud prevention efforts after the pandemic. This is especially so because enhanced communication of fraud mechanisms, regular updates of such emerging risks, and also inclusive participation in fraud preventive strategies have been at their core. The workers have increased the confidence that their respective organizations realize in terms of detecting and mitigating fraud. They participate now in fraud reporting and its prevention more actively than before.

Improved mechanisms of reporting

Organizations have strengthened their reporting mechanisms, making them more accessible and anonymous. Whistleblower hotlines, online reporting mechanisms, and clearly defined escalation procedures have further helped employees report suspicious activities without fear of retaliation. The (ACFE 2022) report shows that organizations with robust reporting mechanisms have a high likelihood of detecting fraud early compared to those without.

Collaboration Across Departments

More importantly, post-pandemic, HR, Finance, and IT departments continued to collaborate in rethinking employee engagement with fraud prevention mechanisms (Ernst & Young, 2021). For example, the HR departments have focused on building integrity within the cultural mindset of an organization, while IT departments have implemented user-friendly reporting and monitoring platforms. This helped ensure that the view on fraud risk from the holistic perspective of one organization was understood down to every aspect. Increasing awareness after the pandemic underpins continuous employee education, strong and articulate communication, as well as effective reporting mechanisms. By actively engaging employees in the fight against the fraud threat, businesses not only have managed to minimize their exposure to various types of risk but have also helped improve the internal culture, essentially accountability and vigilance within their operations (PWC, 2021).

H01: There is no significant difference in the utilization of fraud prevention mechanisms across various departments within organizations.

H11: There is a significant difference in the utilization of fraud prevention mechanisms across various departments within organizations.

- ANOVA test is performed to check the significant difference among the group means.
- Here, the sig. value is 0.00<0.05.
- Hence, we reject the Null hypothesis and conclude that there is a significant difference in the utilization of fraud prevention mechanisms across various departments within organizations.

Table 4.6: ANOVA

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
My department utilizes a comprehensive set of fraud prevention mechanisms.	Between Groups	25.680	5	5.136	8.691	.000
	Within Groups	176.096	298	.591		
	Total	201.776	303			
Fraud prevention mechanisms in my department are regularly reviewed and updated.	Between Groups	15.099	5	3.020	4.723	.000
	Within Groups	190.533	298	.639		
	Total	205.632	303			
There is a formal process for reporting suspected fraud in my department.	Between Groups	18.068	5	3.614	7.990	.000
	Within Groups	134.771	298	.452		
	Total	152.839	303			
My department collaborates with other departments to enhance fraud prevention efforts.	Between Groups	20.606	5	4.121	7.873	.000
	Within Groups	155.996	298	.523		
	Total	176.602	303			
The organization's fraud prevention mechanisms are aligned with industry best practices.	Between Groups	31.626	5	6.325	11.207	.000
	Within Groups	168.187	298	.564		
	Total	199.813	303			

H02: There is no significant difference in the modifications made to fraud prevention mechanisms post-pandemic across organizations.

H12: There is a significant difference in the modifications made to fraud prevention mechanisms post-pandemic across organizations.

- ANOVA test is performed to check the significant difference among the group means.
- Here, the sig. value is 0.00<0.05.
- Hence, we reject the Null hypothesis and conclude that there is a significant difference in the modifications made to fraud prevention mechanisms post-pandemic across organizations.

Table 4.7: ANOVA

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
My department has implemented new fraud prevention measures in response to the COVID-19 pandemic.	Between Groups	12.989	5	2.598	4.208	.001
	Within Groups	183.959	298	.617		
	Total	196.947	303			
The organization has adapted existing fraud prevention mechanisms to better suit remote work environments.	Between Groups	20.111	5	4.022	7.487	.000
	Within Groups	160.087	298	.537		
	Total	180.197	303			
Employees have received training on modifications to fraud prevention measures post-pandemic.	Between Groups	16.939	5	3.388	4.865	.000
	Within Groups	207.505	298	.696		
	Total	224.444	303			
My department has conducted risk assessments to identify new fraud risks post-pandemic.	Between Groups	16.451	5	3.290	6.145	.000
	Within Groups	159.546	298	.535		
	Total	175.997	303			
There has been an increase in the use of technology for fraud prevention since the pandemic.	Between Groups	18.405	5	3.681	6.719	.000
	Within Groups	163.266	298	.548		
	Total	181.671	303			

H03: There is no significant difference in the effectiveness of fraud prevention mechanisms across various departments, both pre- and post-pandemic.

H13: There is a significant difference in the effectiveness of fraud prevention mechanisms across various departments, both pre- and post-pandemic.

- ANOVA test is performed to check the significant difference among the group means.
- Here, the sig. value is 0.00<0.05.
- Hence, we reject the Null hypothesis and conclude that there is a significant difference in the effectiveness of fraud prevention mechanisms across various departments, both pre- and post-pandemic.

Table 4.8: ANOVA

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
The fraud prevention mechanisms in place before the pandemic were effective in mitigating fraud risks.	Between Groups	21.909	5	4.382	7.617	.000
	Within Groups	171.430	298	.575		
	Total	193.339	303			
There were clear procedures for fraud reporting and response before the pandemic.	Between Groups	19.894	5	3.979	7.433	.000
	Within Groups	159.527	298	.535		
	Total	179.421	303			
The organization conducted regular training on fraud prevention before the pandemic.	Between Groups	22.739	5	4.548	6.803	.000
	Within Groups	199.205	298	.668		
	Total	221.944	303			
The incidence of occupational fraud was low prior to the pandemic in my department.	Between Groups	17.441	5	3.488	6.282	.000
	Within Groups	165.477	298	.555		
	Total	182.918	303			
Pre-pandemic fraud prevention measures were aligned with industry standards.	Between Groups	18.738	5	3.748	7.391	.000
	Within Groups	151.101	298	.507		
	Total	169.839	303			
The current fraud prevention mechanisms are more effective than those in place before the pandemic.	Between Groups	16.256	5	3.251	5.925	.000
	Within Groups	163.521	298	.549		
	Total	179.776	303			
Employees have a higher level of confidence in fraud prevention measures post-pandemic.	Between Groups	22.872	5	4.574	9.083	.000
	Within Groups	150.073	298	.504		
	Total	172.944	303			
There is a noticeable decrease in fraud	Between Groups	14.029	5	2.806	3.949	.002
	Within Groups	211.731	298	.711		

incidents since the implementation of post-pandemic measures	Total	225.760	303			
The organization regularly monitors the effectiveness of fraud prevention mechanisms after the pandemic.	Between Groups	18.091	5	3.618	5.689	.000
	Within Groups	189.540	298	.636		
	Total	207.632	303			
Employee engagement in fraud prevention efforts has increased post-pandemic.	Between Groups	24.821	5	4.964	8.076	.000
	Within Groups	183.175	298	.615		
	Total	207.997	303			

H04: There are no commonalities and differences in fraud prevention approaches employed by organizations in different sectors and sizes.

H14: There are commonalities and differences in fraud prevention approaches employed by organizations in different sectors and sizes.

- Regression analysis is performed to test the Relationship among the Variables.
- Here, the sig. The value for both different Sectors and Sizes is 0.00<0.05.
- Hence, we reject the Null hypothesis and conclude that there are commonalities and differences in fraud prevention approaches employed by organizations in different sectors and sizes.

Table 4.9: Model Summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.610[a]	.372	.263	.240

Table 4.10: ANOVA

ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
	Regression	8.853	45	.197	3.424	.000[b]
	Residual	14.938	260	.057		
	Total	23.791	305			

a. Dependent Variable: Do you believe the size of your organization influences its fraud prevention strategies?

Table 4.11: Coefficients

Coefficients

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	1.398	.056		24.984	.000
The fraud prevention mechanisms in place before the pandemic were effective in mitigating fraud risks.	-.024	.038	-.070	-.644	.520
There were clear procedures for fraud reporting and response before the pandemic.	-.014	.042	-.039	-.341	.734
The organization conducted regular training on fraud prevention before the pandemic.	-.092	.043	-.283	-2.170	.031
The incidence of occupational fraud was low prior to the pandemic in my department.	-.049	.038	-.135	-1.283	.201
Pre-pandemic fraud prevention measures were aligned with industry standards.	.084	.041	.226	2.057	.041
The current fraud prevention mechanisms are more effective than those in place before the pandemic.	.019	.042	.052	.450	.653
Employees have a higher level of confidence in fraud prevention measures post-pandemic.	.089	.051	.241	1.738	.083
There is a noticeable decrease in fraud incidents since the implementation of post-pandemic measures	-.015	.037	-.047	-.405	.685

	The organization regularly monitors the effectiveness of fraud prevention mechanisms after the pandemic.	-.016	.042	-.047	-.380	.704
	Employee engagement in fraud prevention efforts has increased post-pandemic.	-.128	.037	-.380	-3.422	.001
	I am aware of the common types of identity fraud that can occur within my organization.	-.038	.031	-.110	-1.213	.226
	I believe that identity fraud poses a significant threat to my organization.	-.010	.032	-.028	-.319	.750
	The organization provides sufficient training on identity fraud awareness.	-.042	.035	-.129	-1.176	.241
	I regularly receive updates on identity fraud trends affecting my industry.	-.025	.030	-.078	-.830	.407
	I feel confident in identifying potential identity fraud scenarios.	.000	.041	-.001	-.011	.991
	I am aware of the warning signs of financial statement fraud in my organization.	.093	.035	.278	2.641	.009
	I understand how expense reimbursement fraud schemes can occur within my department.	.070	.035	.207	2.014	.045
	I am familiar with the techniques used to detect asset misappropriation, such as theft of company resources.	-.067	.036	-.200	-1.876	.062
	I am knowledgeable about the various forms of payroll fraud that can happen, including ghost employees and falsified hours.	-.111	.039	-.324	-2.847	.005

	I can identify behaviors or actions that might indicate vendor fraud, such as inflated invoices or collusion with employees.	-.002	.038	-.004	-.040	.968
	I am aware of the risks associated with procurement fraud, including bid rigging and kickbacks	-.017	.041	-.048	-.419	.675
	I have been trained to recognize potential fraud in expense claims, such as duplicate or inflated submissions.	-.014	.037	-.042	-.377	.707
	I understand how conflicts of interest can lead to fraudulent activities within my organization.	.073	.040	.207	1.807	.072
	I feel confident in reporting suspected occupational fraud through established company procedures.	-.049	.035	-.143	-1.403	.162
	I am aware of the internal controls in place to prevent and detect fraudulent activities in my work area.	.074	.037	.218	1.983	.048
	My department utilizes a comprehensive set of fraud prevention mechanisms.	.043	.045	.127	.965	.336
	Fraud prevention mechanisms in my department are regularly reviewed and updated.	.068	.048	.202	1.424	.156
	There is a formal process for reporting suspected fraud in my department.	.039	.049	.101	.812	.418
	My department collaborates with other departments to enhance fraud prevention efforts.	.024	.041	.065	.584	.560

	The organizations fraud prevention mechanisms are aligned with industry best practices.	-.095	.037	-.277	-2.543	.012
	I am knowledgeable about the fraud prevention mechanisms implemented in my department.	.037	.043	.104	.867	.387
	Employees receive regular training on the organizations fraud prevention policies.	-.041	.044	-.132	-.931	.353
	My organization actively promotes awareness of fraud prevention measures among employees.	.015	.058	.047	.264	.792
	The organization effectively communicates changes to fraud prevention mechanisms.	.062	.045	.194	1.392	.165
	I believe that increased awareness of fraud prevention mechanisms can reduce occupational fraud.	-.062	.037	-.167	-1.665	.097
	My department has implemented new fraud prevention measures in response to the COVID-19 pandemic.	.007	.040	.019	.166	.868
	The organization has adapted existing fraud prevention mechanisms to better suit remote work environments.	-.117	.041	-.322	-2.870	.004
	Employees have received training on modifications to fraud prevention measures post-pandemic.	.013	.037	.039	.342	.733
	My department has conducted risk assessments to identify new fraud risks post-pandemic.	.039	.046	.105	.846	.398

	There has been an increase in the use of technology for fraud prevention since the pandemic.	-.055	.039	-.153	-1.400	.163
	The post-pandemic modifications to fraud prevention mechanisms have been effective in reducing fraud incidents.	-.051	.037	-.147	-1.386	.167
	I feel that the adjustments made to fraud prevention mechanisms have enhanced overall security	.046	.048	.129	.963	.336
	The effectiveness of fraud prevention mechanisms has improved due to recent modifications.	.033	.055	.088	.605	.546
	My department regularly evaluates the success of modifications to fraud prevention measures.	-.057	.044	-.172	-1.283	.201
	Employee feedback is considered when assessing the effectiveness of post-pandemic modifications.	.036	.036	.105	1.017	.310

a. Dependent Variable: Do you believe the size of your organization influences its fraud prevention strategies?

Table 4.12: Model Summary

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.667[a]	.445	.349	.237

Table 4.13: ANOVA

ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	11.679	45	.260	4.630	.000[b]
	Residual	14.573	260	.056		
	Total	26.252	305			

a. Dependent Variable: Do you believe your department manages occupational fraud challenges effectively?

Table 4.14: Coefficients

Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
	(Constant)	1.369	.055		24.781	.000
	The fraud prevention mechanisms in place before the pandemic were effective in mitigating fraud risks.	-.054	.037	-.147	-1.443	.150
	There were clear procedures for fraud reporting and response before the pandemic.	-.054	.041	-.141	-1.314	.190
	The organization conducted regular training on fraud prevention before the pandemic.	-.004	.042	-.011	-.086	.931
	The incidence of occupational fraud was low prior to the pandemic in my department.	-.018	.037	-.048	-.483	.630
	Pre-pandemic fraud prevention measures were aligned with industry standards.	.049	.040	.127	1.222	.223
	The current fraud prevention mechanisms are more effective than those in place before the pandemic.	.038	.041	.100	.928	.354
	Employees have a higher level of confidence in fraud prevention measures post-pandemic.	.100	.051	.257	1.966	.050
	There is a noticeable decrease in fraud incidents since the implementation of post-pandemic measures	.020	.037	.058	.535	.593
	The organization regularly monitors the effectiveness of fraud prevention mechanisms after the pandemic.	.010	.041	.029	.247	.805
	Employee engagement in fraud prevention efforts has increased post-pandemic.	.001	.037	.003	.033	.974

I am aware of the common types of identity fraud that can occur within my organization.	.004	.031	.012	.146	.884
I believe that identity fraud poses a significant threat to my organization.	.023	.032	.059	.729	.467
The organization provides sufficient training on identity fraud awareness.	-.074	.035	-.219	-2.133	.034
I regularly receive updates on identity fraud trends affecting my industry.	.011	.029	.034	.382	.703
I feel confident in identifying potential identity fraud scenarios.	-.135	.041	-.375	-3.302	.001
I am aware of the warning signs of financial statement fraud in my organization.	.100	.035	.283	2.858	.005
I understand how expense reimbursement fraud schemes can occur within my department.	.060	.034	.168	1.745	.082
I am familiar with the techniques used to detect asset misappropriation, such as theft of company resources.	-.067	.035	-.190	-1.895	.059
I am knowledgeable about the various forms of payroll fraud that can happen, including ghost employees and falsified hours.	.004	.039	.010	.097	.923
I can identify behaviors or actions that might indicate vendor fraud, such as inflated invoices or collusion with employees.	.117	.037	.331	3.153	.002
I am aware of the risks associated with procurement fraud, including bid rigging and kickbacks	-.114	.041	-.303	-2.803	.005
I have been trained to recognize potential fraud in expense claims, such as duplicate or inflated submissions.	.100	.037	.282	2.702	.007
I understand how conflicts of interest can lead to fraudulent activities within my organization.	-.005	.040	-.014	-.134	.894

I feel confident in reporting suspected occupational fraud through established company procedures.	-.042	.034	-.118	-1.228	.220
I am aware of the internal controls in place to prevent and detect fraudulent activities in my work area.	-.004	.037	-.012	-.112	.911
My department utilizes a comprehensive set of fraud prevention mechanisms.	-.042	.045	-.116	-.936	.350
Fraud prevention mechanisms in my department are regularly reviewed and updated.	.128	.047	.360	2.707	.007
There is a formal process for reporting suspected fraud in my department.	-.027	.048	-.066	-.570	.569
My department collaborates with other departments to enhance fraud prevention efforts.	-.047	.040	-.122	-1.161	.247
The organization's fraud prevention mechanisms are aligned with industry best practices.	-.027	.037	-.074	-.721	.471
I am knowledgeable about the fraud prevention mechanisms implemented in my department.	-.006	.042	-.016	-.146	.884
Employees receive regular training on the organization's fraud prevention policies.	.018	.044	.055	.412	.681
My organization actively promotes awareness of fraud prevention measures among employees.	-.002	.057	-.006	-.038	.970
The organization effectively communicates changes to fraud prevention mechanisms.	-.056	.044	-.165	-1.266	.207
I believe that increased awareness of fraud prevention mechanisms can reduce occupational fraud.	-.043	.037	-.112	-1.185	.237

	My department has implemented new fraud prevention measures in response to the COVID-19 pandemic.	-.033	.040	-.090	-.819	.413
	The organization has adapted existing fraud prevention mechanisms to better suit remote work environments.	.010	.040	.027	.260	.795
	Employees have received training on modifications to fraud prevention measures post-pandemic.	-.016	.037	-.046	-.421	.674
	My department has conducted risk assessments to identify new fraud risks post-pandemic.	-.088	.045	-.228	-1.949	.052
	There has been an increase in the use of technology for fraud prevention since the pandemic.	-.014	.039	-.037	-.359	.720
	The post-pandemic modifications to fraud prevention mechanisms have been effective in reducing fraud incidents.	-.077	.036	-.213	-2.133	.034
	I feel that the adjustments made to fraud prevention mechanisms have enhanced overall security	.070	.047	.185	1.473	.142
	The effectiveness of fraud prevention mechanisms has improved due to recent modifications.	-.022	.054	-.057	-.417	.677
	My department regularly evaluates the success of modifications to fraud prevention measures.	-.049	.044	-.142	-1.128	.260
	Employee feedback is considered when assessing the effectiveness of post-pandemic modifications.	.037	.035	.102	1.050	.294

a. Dependent Variable: Do you believe your department manages occupational fraud challenges effectively?

4.4 Research Question 3

To what extent have the modifications made to fraud prevention mechanisms post-pandemic been effective in preventing occupational fraud within various departments, and how does this effectiveness differ across departments?

4.4.1 Post-Pandemic Adjustments

The COVID-19 pandemic compelled a sea change in organizations regarding fraud prevention mechanisms to meet the new risks presented by teleworking, operational disruption, and the increasing reliance on technology. These changes were necessary so that adaptation could be made to the newly emerging vulnerabilities created by the rapid changes in the job environment.

How the process of fraud prevention measures adapted to the remote environments of work was, in fact, a huge leap. Traditional internal controls faced challenges related to the segregation of duties as employees donned multiple hats. In response, the organizations enhanced their digital security measures through methodologies such as multi-factor authentication, secure remote access, and virtual monitoring systems that would maintain integrity in distributed work environments.

The second most important adjustment dealt with deeper reliance on advanced technology. Most organizations relied on AI-driven fraud detection systems, machine learning algorithms, and data analytics to find out suspicious activities in real-time. These were quite effective in addressing the growing complication of fraud across the finance and IT sectors.

Organizations also had to upgrade their employee training programs to match the evolution of conditions leading to the fraud risk. Employees were virtually taken through a session aimed at creating awareness about the cyber fraud, vulnerabilities of working from home, and fraud reporting procedures that have changed. This increased the ability of employees to recognize and report fraudulent activities.

Another emphasis was on the increased collaboration between its different departments. Likewise, other functional departments like Finance, IT, and HR began to collaborate to harmonize the fraud prevention mechanism with new operational realities. This includes regular risk assessments, technology upgrades, and cross-functional fraud detection strategies.

These post-pandemic adaptations underline the ability to adapt and collaborate in effective fraud prevention structures that make an entity resilient to fraud risks in the post-pandemic era.

4.4.2 Technological Integration

Advanced technology integration has become the cornerstone of issues relating to the radical change in fraud prevention, especially in light of a number of challenges introduced by the COVID-19 pandemic. It is also trending upwards in the application of innovative tools such as AI, ML, and blockchain in equipping organizations with enhanced detection, prevention, and response capabilities against fraudulent acts.

AI and ML technologies are being highly used in analyzing high volumes of data in near real time, thus providing an organization with the capability for detecting suspicious patterns and anomalies, hence establishing fraud cases more concisely. These are essential tools in sectors that have a great risk, such as finance and IT, where volumes of transactions are large and vulnerabilities can come from most sides. Together with fully automated fraud detection, AI-driven systems reduce human error and increase efficiency.

In doing so, blockchain has equally emerged as a very important tool in fraud prevention, bringing about transparency and accountability into the realm of financial transactions. This is due to its immutable ledger system, which gives very little room for fraud since all transactions are recorded securely and are verifiable. This again goes to seal its importance in industries that demand transaction tracking such as retailing and supply chain management.

Besides, data encryption, multi-factor authentication, and other cybersecurity measures of high standard were taken by organizations in handling remote work vulnerabilities. These tools protect sensitive data from unauthorized access and maintain compliance with regulatory standards set.

These advantages are offset by the challenges in implementing these technologies, including high costs, with many detecting possible false positives in fraud detection. More particularly, the scale and resource constraints make it difficult for the smaller organizations to adopt such tools. In sum, technological integration has massively enhanced the fraud prevention capability by availing sophisticated solutions to run side by side with evolving threats and emphasizing the importance of continuous investment in adaptation.

4.5 Research Question 4

What commonalities and differences exist in the approaches to fraud prevention among organizations of different sizes and in different sectors, and how can these variations inform the development of targeted, department-specific strategies to enhance overall organizational resilience against occupational fraud?

Sectoral Differences

The financial industry is one of the most regulated industries, where developed technologies such as AI and machine learning are deployed in real-time monitoring of transactions to keep them in compliance with the laws on AML and the Sarbanes-Oxley Act. These tools help identify abnormalities in the vast number of transactions that happen daily, but the complexity of financial systems makes fraud prevention an eternal cat-and-mouse game. Similarly, cybersecurity is a concern in the IT industry, which deploys various methods like firewalls, multi-factor authentication, encryption protocols, and intrusion detection systems. The sector always remains under the threat of data breaches and system exploitation, and this requires monitoring of the network 24*7 with the use of advanced analytics.

The major problems this industry faces are payment fraud, return fraud, and inventory theft. Fraud detection systems integrated with the POS and online payment processing system of retailers help detect frauds. Most of the tokenization and encryption technologies for keeping customer data secure, particularly in the ever-expanding e-commerce space, have been widely adopted. Meanwhile, the health sector addresses industry-specific fraudulent risks related to billing and insurance fraud requiring forensic accounting and compliance audits. Another important priority area now is the security of electronic health records against data breaches.

Manufacturing practices focused on fraud prevention, more so in procurement and the mismanagement of inventory levels, involve vendors' audit verification and the analysis of supply chain performance. These are empowered through technologies such as-but not limited-to-blockchain and RFID tracking, toward bringing transparency and accountability into all transactions. Despite these differences, each sector also shared a number of common best practices that included the use of technology, employee training programs, and internal controls to help build a culture resistant to fraud. These sector-of-interest perspectives point to targeted strategies for individual industries but also reiterate across all sectors an imperative of collaboration to enhance overall organizational resilience in fraud risk.

Organizational Size

Actually, through both the previous and current generation, the size of organization remains a key determinant when it comes to fraud combating. Large organizations with diverse heavy masses for resources and complexity in construction are more capable of performing sophisticated tools: artificial intelligence deployment, machine learning, or blockchain. These technologies involve real-time fraud detection enabled by the processing of terabytes of data for mismatches. Large organizations usually have very strong internal controls, such as the "three lines of defense": operational management, risk management, and audits. A special compliance department follows strict regulatory rules and regulations, for example, SOX for financial reporting or HIPAA for security of healthcare data. On the downside, the complexity of a large organization creates problems of coordination among many departments, plus managing costs that can be extremely high using advanced technologies.

Smaller organizations, on the other hand, rely on inexpensive and manual controls because of limited resources. Examples of such controls are basic internal controls like the separation of duties, cash flow monitoring, and less frequent audits. Low-cost fraud detection tools with existing systems, such as point-of-sale systems, usually detect suspicious transactions in most small firms. Employee involvement is very necessary for these firms since well-trained employees are usually the first line of defense. Moreover, small organizations may outsource forensic audits or even resort to third-party experts in dealing with complex fraud risks. While these steps are effective within their own domain, smaller organizations tend to be more vulnerable to fraud because of minimal internal control and a relatively fewer number of technological integrations.

While there are such factors that differentiate large organizations from their smaller counterparts, both use the same practices of promoting organizational accountability, anonymous reporting systems, and employee training. To nurture resilience, large organizations can focus on collaboration between groups, while the smaller version can adopt specific, efficient resource strategies. Eventually, it is important for the organization, no matter big or small in size and nature, to work its way toward a full-scale plan of fraud deterrence capable of balancing operation feasibility against comprehensive risk mitigation.

4.5.1 Training Gaps and Recommendations

Actually, through both the previous and current generation, the size of organization remains a key determinant when it comes to fraud combating. Large organizations with diverse heavy masses for resources and complexity in construction are more capable of performing sophisticated tools: artificial intelligence deployment, machine learning, or blockchain. These technologies involve real-time fraud detection enabled by the processing of terabytes of data for mismatches. Large organizations usually have very strong internal controls, such as the "three lines of defense": operational management, risk management, and audits. A special compliance department follows strict regulatory rules and regulations, for example, SOX for financial reporting or HIPAA for security of healthcare data. On the downside, the complexity of a large organization creates problems of coordination among many departments, plus managing costs that can be extremely high using advanced technologies.

Smaller organizations, on the other hand, rely on inexpensive and manual controls because of limited resources. Examples of such controls are basic internal controls like the separation of duties, cash flow monitoring, and less frequent audits. Low-cost fraud detection tools with existing systems, such as point-of-sale systems, usually detect suspicious transactions in most small firms. Employee involvement is very necessary for these firms since well-trained employees are usually the first line of defense. Moreover, small organizations may outsource forensic audits or even resort to third-party experts in dealing with complex fraud risks. While these steps are effective within their own domain, smaller organizations tend to be more vulnerable to fraud because of minimal internal control and a relatively fewer number of technological integrations.

While there are such factors that differentiate large organizations from their smaller counterparts, both use the same practices of promoting organizational accountability, anonymous reporting systems, and employee training. To nurture resilience, large organizations can focus on collaboration between groups, while the smaller version can adopt specific, efficient resource strategies. Eventually, it is important for the organization, no matter big or small in size and nature, to work its way toward a full-scale plan of fraud deterrence capable of balancing operation feasibility against comprehensive risk mitigation. Given that firms have been working to enhance employees' knowledge and training since the outbreak of COVID-19, this survey indicated many areas of optimization yet to be effected at the level of training in an organization. These gaps become important in highlighting ways an organization could strengthen its policies and strategies more succinctly on fraud prevention and detection CERT-In. (2021).

One such lacuna exists regarding the limited focus on emerging fraud risks. While most of the training programs still lay emphasis on conventional issues, such as asset misappropriation and financial statement fraud, newer threats such as cyber fraud, phishing scams, and ransomware attacks have been greatly neglected. It is direly needed that such skills be imparted to the employees with increased adoption of digital tools and a remote work environment. Without this emphasis, significant vulnerabilities remain within the workforce.

There was also a lot of inconsistency in training between departments. Finance and IT departments often get very frequent, specialized training in matters pertaining to their job responsibilities, while other departments, such as HR and Operations, may not. The result is that some teams may not be prepared to recognize and handle risks particular to their role, which can make an organization's overall fraud prevention strategy vulnerable.

Another critical issue is the dependence on passive learning approaches, including non-interactive lectures or static reading materials. Most programs lack practical, scenario-based exercises or real-life case studies that would help employees recognize and respond to fraud risk better. Interactive approaches, such as role-playing or simulations, are not used often enough, even though it has been proven that such approaches reinforce learning and improve retention accordingly.

Another area of concern is employee engagement in training programs. Most participants do not find the sessions very interactive or relevant to their job, which eventually diminishes their interest in participating in the training or implementing what they learned. Organizations have to engage their programs to be more engaging and job-specific so it will be relevant to every employee.

Organizations can, therefore, fill such gaps in their curricula with state-of-the-art fraud topics such as cybersecurity threats and insider risks. Departmentalized training is also something that should be introduced. The idea is to make different teams aware of the problems they specifically face. For instance, HR may be taught about ethical hiring practices while the IT department concentrates on sophisticated cybersecurity measures. Similarly, regular updates and refresher courses need to be imparted to update employees with changing fraud tactics and policies.

Besides this, training programs need to include more interactive approaches, such as simulations and gamified learning. These methods are not only more interesting for employees, but they can also show how theoretical knowledge may work in a real-life situation. The implementation of feedback will help an organization find the weakest points in its training and further improve it.

Practical Implications

The findings bring recommendations for organizational leaders on the necessity of targeted training, investment in technology, and collaboration between departments as means of strengthening fraud prevention. This would include designing the training to address specific risks in every department and changing trends of fraud to build a workforce that is vigilant. Other investments involve advanced technologies like AI and blockchain that are going to help improve fraud detection and facilitate efficiency. Furthermore, enabling collaboration between the Finance, IT, and HR departments provides an integrated approach to mitigating the risks of fraud. All these measures put together will reinforce the resilience of the organization, make it less vulnerable, and create a culture of accountability within it.

Summary of findings

This fraud prevention mechanism has turned out to be very diverse among the various departments, industries, and size of the organizations. While some departments, such as Finance and IT, use sophisticated technologies like AI and blockchain, other departments focus more on compliance, training, and awareness. In the post-pandemic period, an increased adaptation of organizations with technological integration and adapting fraud measures to the remote work challenge was noted; training was more focused and directed to new fraud risks, such as cyber threats. This usually meant that very large entities, as perhaps expected, enjoyed extensive resources in respect of sophisticated controls, while smaller businesses made use of strategies focused on cost efficiency with hands-on fraud prevention. Such findings emphasize how the use of unique, department-focused approaches goes all the way to fully embracing fraud prevention strategies.

Conclusion

The studies undertaken here have shown that a blend of technological, procedural, and cultural solutions is appropriate in varying departments, sectors, and sizes of organizations with varying specific risks. Technological development and interdepartmental cooperation, along with the post-pandemic situation, has substantially improved resiliency towards occupational fraud. Post-pandemic adjustments give more emphasis to the enhanced cybersecurity feature, including multi-factor authentication and AI-driven fraud detection systems, with virtual training programs devoted to emerging risks like cyber fraud. On the other hand, management faces difficulties in increasing awareness of these frauds due to insufficient training; thus, such training programs should be interactive. It helps organizations reduce the risk of fraud by institutionalizing accountability, infusing advanced technologies, and promoting cross-functional collaboration. It also indicates in the analysis that there are varying levels of fraud, depending on the organization size, ranging from disproportionately bigger losses of small organizations to massive ones having more limited resources, and to even huge ones employing advanced technologies like blockchain and AI in mitigation processes but dealing with systemic complexities. Such steps will not only ensure readiness against any emerging fraud tactics but also help in sustaining organizational integrity.

CHAPTER V: DISCUSSION

5.1 Discussion on Research Question One

What are the key fraud prevention mechanisms currently employed by organizations, and how do these mechanisms vary across different departments, including HR, Accounting, Finance, Operations, IT, and other relevant departments?

The study showed large discrepancies across departments in the organization with regard to the adoption and success of fraud prevention mechanisms, and thus the need for differentiation. Finance and IT were two identified departments that are the most integral parts of fraud prevention, making use of advanced technologies such as AI, machine learning, to carry out anomaly and pattern identification typical of fraud. This also aligns with what is represented in the literature, where advanced analytics has been core in realizing improvements in fraud detection capabilities, Kassem & Turksen, (2021). Finance departments, for instance, have a strong focus on regulatory compliance standards like SOX and also set up solid internal audits that act as backbone for organizational fraud prevention.

While cybersecurity concerns make the IT department emphasize protection methods, such as encryption or multi-factor authentication of sensitive information against breaches, findings support past studies like that of Zhu et al. 2021, which reported IT department plays a crucial role in mitigating risks from fraudulent activities enabled through technology; thus, transaction integrity rests assured with accuracy of the financial reporting and true consideration to its internal controls from the account department.

Smaller departments, including HR and Marketing, have supporting but critical roles. HR implements corporate ethics through training programs and sensitization that minimize risks of collusion or rationalization in the theory of the Fraud Triangle by Mansor & Abdullahi, (2015). Marketing departments, on the other hand, are concerned with securing digital interactions and protecting consumer information, especially in those industries prone to payment fraud.

The ANOVA analysis indicates significant differences between the departments regarding the use and effectiveness of fraud prevention mechanisms. These differences indicate that departmental strategies need to be designed in light of unique risks and responsibilities.

Findings also signal the need for cross-departmental collaboration to create a unified, resilient organizational framework against occupational fraud.

5.2 Discussion on Research Question Two

How have organizations modified their fraud prevention mechanisms in response to the global pandemic, and what specific adaptations have been made post-pandemic to enhance resilience against occupational fraud?

The COVID-19 pandemic brought tremendous and profound changes in organization strategies and principles of fraud prevention. Traditional mechanisms, such as audits pursued episodically, were patently incapable of responding to these emerging vulnerabilities of a new class brought about by working at home. In response, advanced digitization security measures were adopted, comprising multi-factor authentication and virtual monitoring systems. This shift aligns with the insight of Levi and Smith, (2022) that "there was increased dependence upon cybersecurity protocols during the pandemic period".

The integration of AI-driven fraud detection systems and machine learning algorithms formed the backbone of post-pandemic adaptations. These solutions offered the ability to track all transactions in real time, hence identifying suspicious activities with more effectiveness than ever, thanks to the challenges introduced by the decentralization of workflows. Previous studies, such as Zhu et al. (2021), have identified how AI could help in mitigating fraud risks, especially in transaction-intensive industries like finance and IT.

The enhancement of employee training programs was another significant change. Virtual training sessions on emerging fraud risks, such as phishing and cyber scams, raised fraud awareness through a proactive culture. This finding is supported by studies like McCormack (2022), which have established the role of targeted training in empowering employees to act as the first line of defense in occupational fraud.

Cross-functional collaboration was one of the post-pandemic strategies. Functions such as Finance, IT, and HR collaborated to align fraud prevention mechanisms with the new operational realities. This also corroborates a report by Ernst & Young (2021) that cited the benefits accruing from integrated approaches to fraud risk management. These adaptations underlined the resilience and adaptiveness of organizations in mitigating occupational fraud risks in a rapidly changing environment.

5.3 Discussion on Research Question Three

To what extent have the modifications made to fraud prevention mechanisms post-pandemic been effective in preventing occupational fraud within various departments, and how does this effectiveness differ across departments?

The changes in the fraud prevention mechanism after the pandemic have remarkably improved the effectiveness, though with significant variations in departments. Finance and IT departments were the biggest beneficiaries of the changes in post-pandemic fraud prevention mechanisms. Advanced technologies including AI and blockchain enhanced their fraud detection and prevention in real time. This finding is supported by research by Suh et al. (2019), who noted that technology enhances the effectiveness of internal controls and increases fraud detection capabilities.

It illustrated the use of AI in finance departments to monitor high-volume transactions, therefore reducing time spent responding to anomalies. The IT department utilized advanced analytics and block-chain for the enhancement of data security by locating vulnerabilities within the networks. These advancements meet and address the increased sophistication within the fraud schemes throughout the pandemic Lang et al., (2023).

In contrast, support functions such as HR and Operations realized relatively small improvements due to the absence of specialized training and resources. While HR was instrumental in driving ethical practices and understanding, it was sometimes hampered by spotty training programs. Operations, which is responsible for procedural adherence, benefited from new, enhanced workflows but did not have enabling technologies as Finance and IT did.

The changes were also not effective in the level of involvement and training of employees. The ANOVA results reveal a significant increase in employee confidence to participate in the prevention of fraud post-pandemic. This supports findings by PWC (2021), that place strong emphasis on the need for inclusive training programs as well as robust reporting mechanisms in building an organization's resilience.

While these steps have been taken, challenges persist, especially at the level of smaller departments that are usually under-resourced and with limited access to resources and technology. The findings call for an ongoing investment in training and technology, appropriate to each department's needs, as mechanisms for fraud prevention cannot function optimally without this.

5.4 Discussion on Research Question Four

What commonalities and differences exist in the approaches to fraud prevention among organizations of different sizes and in different sectors, and how can these variations inform the development of targeted, department-specific strategies to enhance overall organizational resilience against occupational fraud?

The study indicated that different organizations, in terms of size and sector, approach fraud prevention differently, but all are the same at the foundation, which is internal controls and employee training. The large organizations with big systems and enough resources use sophisticated tools in fraud detection, including AI, blockchain, and machine learning. This will give them the ability to monitor the activities in real time and thus respond faster, which corroborates the findings of Mansor and Abdullahi (2015).

Smaller ones, however, rely on affordable methods such as manual controls, job separation, and periodic monitoring of cash flow. While unsophisticated, these practices befit their limited resources. This agrees with Davis, 2019, who opines that the key to effective fraud prevention in SMEs lies in targeted and low-cost strategies.

Sectoral differences are yet another factor that shapes fraud prevention approaches. For example, the financial sector focuses on compliance issues and uses advanced analytics in tracking transactions, as Kalovya 2023 presents. In the IT sector, cybersecurity with encryption and multi-factor authentication is considered paramount in view of the increasing data breaches. Retail sectors focus on tokenization and encryption in securing customer data, while manufacturing focuses on supply chain transparency through blockchain and RFID tracking. These findings are supported by a study conducted by Levi and Smith in 2022, which outlined that fraud risks are sector-specific.

Yet, despite such contrasts, practices like whistleblower hotlines, ethical training programs, and collaboration across departments were common in organizations of all sizes. It is shared strategies like these that form the basis for the call for a culture of accountability and vigilance. The findings indicate the necessity for focused, departmental strategies in consideration of sectoral risks and organizational capacities. While large organizations should be concerned with interdepartmental collaboration and integration of technology, smaller firms are in a position to implement tailored training programs and partnerships with third-party experts. These approaches enhance organizational resilience and ensure the scalability and sustainability of fraud prevention mechanisms.

5.5 Conclusion

The discussion of results further emphasizes the multi-faceted nature of fraud prevention mechanisms, thus making it necessary for tailored approaches to meet various challenges related to different departments, sectors, and organizational sizes. It was identified that the Finance and IT departments play the key roles in fraud prevention with the use of advanced technologies like AI and machine learning, while the HR department contributes to creating an ethical and aware culture through selected training programs. Sectoral differences further bring the review of how industry risks are shaping fraud strategies among various industries: financial ones comply with regulatory requirements, while others take care of data security, such as healthcare institutions.

But also with better cybersecurity, advanced analytics, and virtual training programs, some clear signs are that post-pandemic adaptations have served to entrench organizational resilience against the fraudster. However, gaps remain in how well training is carried out across departments and readiness and ability to access advanced tools at various levels of an organization, smaller ones included. These weaknesses give rise to a continuing need for investment in technology, customized training programs, and cross-functional collaboration.

The findings finally pinpoint that successful fraud combating strategies have a need for technological, procedural, and cultural interventions. Reducing emerging risks and embedding proper employee engagement and behavior fosters a proactive anti-fraud stance in organisations and helps construct mechanisms with strength in integrity and resilience during changes of any kind in fraudulent attacks on fraud. These processes would remove potential vulnerabilities that come about while increasing their effectiveness toward preventing fraud cases.

CHAPTER VI: SUMMARY, IMPLICATIONS AND RECOMMENDATIONS

6.1 Introduction

This chapter summarizes the significant findings of the study with implications for organizations and policy makers. It reflects upon how anti-fraud controls match up to the occupation fraud that has been realized, in particular, sectoral differences, organizational size, and post-pandemic adaptations. Based on empirical evidence, the chapter outlines the theoretical and practical contributions that provide actionable recommendations to overcome the gaps identified in fraud prevention mechanisms.

The chapter has demonstrated how much cutting-edge technologies (AI and machine learning), among others, have reinforced the process of fraud detection in areas like finance or IT. This work comments on the proposal of Singh (2020) related to the creation of cultural awareness for ethics and accountability-a culture that would be formed through regular training programs suited to the needs of certain departments. The study also outlays the importance of both intra- and interdepartmental collaboration in adapting to changing fraud risks, especially now with the post-pandemic situation.

Additionally, the chapter explores organizational size as a factor affecting fraud prevention strategy design and implementation; whereas large organizations apply sophisticated tools in their fraud prevention strategies, small firms focus on affordable and manual controls only. In this way, the chapter identifies the road to improvement regarding fraud prevention strategies for building resilience against occupational fraud in various organizational settings.

6.2 Summary of the Study

The anti-fraud controls of occupational fraud with regard to sectoral and departmental variations, organizational size, and post-pandemic adaptations were assessed in this study. It noted that fraud prevention mechanisms have been varying among the different departments, and there the finance and IT departments remain at the forefront as they are very proactive and eager to implement advanced technological solutions in the form of AI, machine learning, and blockchain. While such technologies improved real-time fraud detection and reduced the levels of vulnerabilities, especially within those areas with high volume transactions and intricacy of operations, in 2023 Efijemue et al. made sure that less technologically engaged departments like HR and Operations contribute by maintaining ethical culture and procedural compliance accordingly. The study also found sectoral differences in fraud risks and prevention strategies.

For example, the financial sector is concerned with regulatory compliance and transaction monitoring, while the retail sector addresses payment fraud and inventory theft through integrated fraud detection systems Levi & Smith, (2022). In the same way, the size of the organization determines the resources and tools available for fraud prevention. Large organizations use advanced internal controls such as the "three lines of defense," while small firms use manual approaches and third-party audits Mwangi & Ndegwa, (2020). The adjustments to anti-fraud mechanisms were more immense post-pandemic: the addition of virtual employee training, increased cybersecurity, and a greater reliance on analytics driven by AI. These are all indicative of increased fraud risk awareness and resiliency across departments, according to Levi & Smith (2022). This thus implies that integrated technological, procedural, and cultural solutions are paramount if the fight against fraud is to eventually overcome the emerging risks and organizational constraints underlined.

6.3 Implications

The findings of this study have important theoretical and practical implications for understanding and combating occupational fraud. Theoretically, this study reiterates the already developed frameworks of the Fraud Triangle and Fraud Diamond in underlining how the interplay between opportunity, pressure, and rationalization in shaping fraud risks across different organizational contexts. This research underlines the contextual factors such as sectoral variations, departmental roles, and organizational size in shaping fraud prevention strategies and enriches the body of literature on fraud mitigation.

Practically, it brings actionable insights for organizational leaders as well as policymakers. First, the findings have emphasized the transforming role of advanced technologies such as AI and blockchain in fraud prevention, especially within high-risk industries like finance and IT, by Zhu et al. (2021). In this regard, it provides the ability for organizations to detect abnormalities in real time with these tools, thus further lowering the incidence of occupational fraud.

This is again upheld by the fact that one finds department-specific methods quite necessary for fraud prevention-the peculiar challenges and operationally vulnerable areas in every department are different. For example, the Finance departments would be requiring highly stringent compliance and monitoring systems, while in the HR, efforts should be nurtured more on ethical organization culture. Indeed, adaptations during and after the pandemic proved just the same thing-the extent to which continuous learning from ongoing changes and collaboration at departments and outside of it exist, added by measures with the help of digital security or virtual training programs. Such studies indicate that the fraud risk is reduced when there is employee involvement and cross-functional teams.

It provides a way of developing resilient anti-fraud frameworks across diverse organizational contexts by combining technologically advanced solutions with bespoke training and organizational collaboration.

6.4 Suggestions

Based on the facts of this study, a few suggestions that could be targeted may help key stakeholders and policy framers in strengthening fraud prevention mechanisms within an organization. These recommendations relate to sector-specific strategies, technology integration, and employee-centric approaches toward occupational fraud.

Policymakers should take a leaf from this study: encouraging measures in the application of state-of-the-art technologies such as AI and blockchain contribute to fraud detection capability enhancement. These instruments have successfully been used to offer real-time monitoring and anomaly detection in high-risk sectors such as finance and IT, according to Zhu et al., (2021). This may require updates within the regulatory framework. These updates ought to be considerate towards enabling such kinds of technologies. Standards will also be subject to review in terms of compliance on fraud prevention.

Leaders are advised to develop department-specific strategies to control certain types of unique fraud risk factors. In the finance department, internal fraud controls would revolve around internal controls and audits, while in IT, there is a need to institute cybersecurity needs including multi-factor authentication and encryption of data Efijemue et al., (2023). Human resources would drive a strong ethics culture through good employee training programs.

The study has recommended virtual training programs and interdepartmental collaboration in the post-pandemic situation to deal with the emerging fraud risks. Regular risk assessment and updating of fraud prevention mechanisms are needed to keep the resilience of organizations not lagging behind the evolution of fraud threats. As per Mwangi & Ndegwa, (2020), low-budget fraud control measures such as manual controls, third-party audits, and a basic fraud detection system can be afforded by smaller organizations that lack substantial resources.

It is expected that recommendations on how to build robust and scalable anti-fraud frameworks are made and that any organization, no matter the sector or size, will be resilient toward occupational fraud in all aspects while promoting accountability and vigilance.

6.5 Scope for Further Research

The contribution of this present study has underlined the several dimensions of occupational fraud and thus emphasized the need for anti-fraud mechanisms tailored to suit specific contexts. There are, however, some grey areas that have not been touched upon and call for further research to advance the understanding and prevention of fraud in organizational settings.

Although this study targeted fraud prevention across sectors and departments, further research could give greater detail on the role of emergent technologies such as AI and blockchain. Work by Zhu et al. reveals that although such tools have indeed shown bright prospects, further research is required into the challenges presented in implementing these technologies, particularly by those organizations with limited resources.

Second, this present research has placed more focus on fraud prevention mechanisms which have changed after the pandemic. Future research might be done with a longitudinal design to assess any long-term effects of those changes and their effectiveness in controlling occupational fraud over a period of time. Other work could explore in greater depth the interaction of fraud risks and emerging trends in the workplace, such as hybrid working, to provide practical insights.

Third, though there had been discussions of the implementation of training programs considered one of the very substantial elements in fraud prevention, further research is still called for in order to be able to optimize these. This might include research into whether newer approaches to training could facilitate an anti-fraud culture, such as gamified learning or using real-world simulations.

Lastly, comparative studies between developed and developing economies could be used to provide insight into the contextual factors influencing fraud prevention strategies. Identification of these gaps, therefore, can be a basis upon which further studies can go ahead to develop holistic, scalable solutions for combating occupational fraud in various organizational and cultural contexts.

6.6 Conclusion

This chapter provides an overview of some key findings, implications, and actionable recommendations derived from this study on anti-fraud controls, affecting the incidence of occupational fraud. The research emphasized the necessity of a technological advancement combined with procedure-based approaches, besides the cultural intervention measure while developing the required initiatives for fraud possibilities at a minimum. There started departments like Finance and IT, which played a very important role with advanced tools for AI and blockchain fraud detection in real time, as was emphasized by Zhu et al. (2021). In the meantime, the HR and Operations Departments try to create ethical environments and compliance with the rules and policies of the company, according to Singh (2020).

The post-pandemic landscape has demanded some significant adaptations in the way that cybersecurity is managed, virtual training programs are run, and departments collaborate-reflecting the growing complexity of fraud risks in an increasingly digitally reliant world. These findings suggest that fraud prevention strategies need to be differentiated according to the particular challenges facing individual sectors and organization sizes.

The implications of this study go to the policymakers, organizational leaders, and increased adoption of innovative solutions in addition to promoting a proactive anti-fraud culture. Nevertheless, some of the limitations that still linger include the limited access to advanced technology by smaller organizations and inconsistent training across departments. Therefore, future research should fill in these gaps through the investigation of longitudinal effects of emerging trends in the workplace and global differences in how fraud prevention strategies are adopted.

The study advocates for fraud prevention mechanisms that need to evolve continuously so that achieving organizational resilience can be considered. Organizations could protect their integrity and reduce their vulnerabilities through comprehensive, collaborative, and adaptive.

APPENDIX A
SURVEY COVER LETTER

I am conducting research on "Exploring the Impact of Anti-fraud Controls on Occupational Fraud".

The primary objective of this questionnaire is to obtain relevant information from different employees currently working in different roles in the organisation. Occupational fraud is a term used to describe fraudulent activities committed by employees, management, or third parties against an organisation. Anti-fraud controls are procedures and policies designed to prevent, detect, and respond to fraudulent activities within an organization.

I humbly request you to please spare a few minutes from your precious time to help me in the study.

This is an online survey (Google form) and does not collect any personal identification details and your response will be purely confidential, anonymous, and used only for the specific purpose of supporting the research.

I eagerly anticipate your insights and express sincere thanks to you in advance for contributing your valuable time and inputs.

APPENDIX B

INFORMED CONSENT

I have gone through the information provided and I am willing to participate in the survey. I understand that by completing this questionnaire I am consenting to be part of the research study.

REFERENCES

1. Abu Amuna, Y.M. and Abu Mouamer, F., 2020. Impact of applying fraud detection and prevention instruments in reducing occupational fraud: case study: ministry of health (MOH) in Gaza Strip. *International Journal of Advanced Studies of Scientific Research*, *4*(6).
2. Almalki, K., 2022. *Factors engendering corporate fraud and mechanisms for enhancing the detection and prevention of fraudulent financial practices in the UK retail industry* (Doctoral dissertation, University of Sheffield).
3. Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F., 2023. Development of a multi-objective's integer programming model for allocation of anti-fraud capacities during cyberfraud mitigation. *Journal of Financial Crime*, *30*(6), pp.1720-1735.
4. Aye, S.T., 2023. *Internal Control Practices, Fraud Prevention And Financial Performance of" A" Bank* (Doctoral dissertation, MERAL Portal).
5. Altamimi, H., Liu, Q. and Jimenez, B., 2023. Not too much, not too little: Centralization, decentralization, and organizational change. *Journal of Public Administration Research and Theory*, *33*(1), pp.170-185.
6. Alawida, M., Omolara, A.E., Abiodun, O.I. and Al-Rajab, M., 2022. A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University-Computer and Information Sciences*, *34*(10), pp.8176-8206.
7. Association of Certified Fraud Examiners (ACFE). 2022. *Report to the nations: Occupational fraud and abuse.*
8. Abu Amuna, Y.M. and Abu Mouamer, F., 2020. Impact of applying fraud detection and prevention instruments in reducing occupational fraud: case study: ministry of health (MOH) in Gaza Strip. *International Journal of Advanced Studies of Scientific Research*, *4*(6).
9. Al-Ababneh, M.M., 2020. Linking ontology, epistemology and research methodology. Science and Philosophy, 8(1), pp.75-91.
10. Alayli, S., 2022. The impact of internal control practices on fraud prevention: The case of Lebanese small-medium enterprises. *European Journal of Business and Management Research*, *7*(5), pp.141-147.

11. Alharahsheh, H.H. and Pius, A., 2020. A review of key paradigms: Positivism VS interpretivism. Global Academic Journal of Humanities and Social Sciences, 2(3), pp.39-
12. Allan, G., 2020. Qualitative research. In Handbook for research students in the social sciences (pp. 177-189). Routledge.
13. Allan, M., Rangarajan, N. and Shields, P., 2021. The potential of working hypotheses for deductive exploratory research. Quality & Quantity, 55(5), pp.1703-1725.
14. Agwor, T. C. 2017. Fraud prevention and business performance in quoted manufacturing companies in Nigeria. *European Journal of Accounting Auditing and Finance Research*, *5*(9), 71-80.
15. Akuh, C. G. 2017. Small retail business strategies to detect and prevent employee fraud.
16. Alayli, S. 2022. The impact of internal control practices on fraud prevention: The case of Lebanese small-medium enterprises. *European Journal of Business and Management Research*, *7*(5), 141-147.
17. Alcobary, M. 2022. *Strategies that Retail Business Owners Use to Prevent and Reduce Employee Theft* (Doctoral dissertation, Walden University).
18. Ahmad, A.H., Masri, R., Zeh, C.M., Shamsudin, M.F. and Fauzi, R.U.A., 2020. The impact of digitalization on occupational fraud opportunities in the telecommunication industry: a strategic review. *PalArch's Journal of Archaeology of Egypt/Egyptology*, *17*(9), pp.1308-1326.
19. Albrecht, W.S., Albrecht, C.O., Albrecht, C.C. and Zimbelman, M.F., 2006. Fraud examination (p. 696). New York, NY: Thomson South-Western.
20. Albrecht, W. S., Albrecht, C. O., & Albrecht, C. C. 2012. Fraud examination. Cengage Learning.
21. Anderson, R., Barton, C., Böhme, R., Clayton, R., Ganán, C., Grasso, T., Levi, M., Moore, T. and Vasek, M., 2019, June. Measuring the changing cost of cybercrime. In *The 18th Annual Workshop on the Economics of Information Security (WEIS 2019)*.
22. Anderson, J., Durbin, S., & Salinger, S. 2021. Cybersecurity: risk management in the era of digital disruption. Journal of Business and Technology, 5(3), 112-131.
23. Association of Certified Fraud Examiners (ACFE). 2019. Report to the nations on occupational fraud and abuse. ACFE.
24. Association of Certified Fraud Examiners (ACFE). 2021. The COVID-19 pandemic's impact on occupational fraud risks. ACFE.

25. Association of Certified Fraud Examiners (ACFE). 2021. Report to the nations on occupational fraud and abuse. ACFE.
26. Bianchi, L. 2021. Exploring ways of defining the relationship between research philosophy and research practice. 28(113), pp.31-50.
27. Baldwin, A. A., & DiGabriele, J. A. 2018. Forensic accounting in the era of big data. Journal of Forensic and Investigative Accounting, 10(2), 231-247.
28. Bierstaker, J. L., Brody, R. G., & Pacini, C. 2006. Accountants' perceptions regarding fraud detection and prevention methods. Managerial Auditing Journal, 21(5), 520-535.
29. Button, M., & Cross, C. 2020. The impact of COVID-19 on cybercrime and fraud in Australia. Crime, Law, and Social Change, 74(4), 299-317.
30. Beemamol, M. 2023. Occupational Fraud in the Highly Regulated Banking Industry: The Case of India. In *Concepts and Cases of Illicit Finance* (pp. 175-203). IGI Global
31. Bello, O.A. and Olufemi, K., 2024. Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. *Computer Science & IT Research Journal*, *5*(6), pp.1505-1520.
32. Baba, L.L., 2019. *Effectiveness of forensic accounting services in financial crime detection and prevention in selected Public organizations in Dar Es Salaam Tanzania* (Doctoral dissertation, Kampala International University, College of Economics & management.).
33. Bonrath, A. and Eulerich, M., 2024. Internal auditing's role in preventing and detecting fraud: An empirical analysis. *International Journal of Auditing*, *28*(4), pp.615-631.
34. Buabeng, A.A., 2020. *A comparative case study of internal controls and the impact of fraud on nonprofit organizations*. Northcentral University.
35. Bello, O.A. and Olufemi, K., 2024. Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. *Computer Science & IT Research Journal*, *5*(6), pp.1505-1520.
36. Banerjee, R., 2024. *Corporate Frauds: Now Bigger, Broader and Bolder*. Penguin Random House India Private Limited.
37. Bojilov, M., 2023. *Methods for assisting in detection of synthetic identity fraud in credit applications in financial institutions* (Doctoral dissertation, CQUniversity).
38. Biegelman, M.T. and Bartow, J.T., 2012. *Executive roadmap to fraud prevention and internal control: Creating a culture of compliance*. John Wiley & Sons.
39. Bolton, R.J. and Hand, D.J., 2002. Statistical fraud detection: A review. *Statistical science*, *17*(3), pp.235-255.

40. Bishop, D.Y., 2022. *Fraud Risk Management to Detect and Prevent Employee Fraud in Small Rural Businesses*. Liberty University.
41. Banerjee, R., 2024. *Who Cheats and How: Scams, Frauds and the Dark Side of the Corporate World*. Penguin Random House India Private Limited.
42. Babaei, K., Chen, Z. and Maul, T., 2019. A Study of Fraud Types, Challenges and Detection Approaches in Telecommunication. *Journal of Information Systems and Telecommunication*, *7*(4), pp.248-261.
43. Bartsiotas, G.A. and Achamkulangare, G., 2016. Fraud prevention, detection and response in United Nations system organizations. *Jenewa: United Nations*.
44. Bodker, A., Connolly, P., Sing, O., Hutchins, B., Townsley, M. and Drew, J., 2023. Card-not-present fraud: using crime scripts to inform crime prevention initiatives. *Security Journal*, *36*(4), pp.693-711.
45. Bhargava, V., 2024. Reflections on World Bank engagement in governance and anticorruption: insider and outsider perspectives. In *The Elgar Companion to the World Bank* (pp. 359-371). Edward Elgar Publishing.
46. Chidiebere Chibuike. 2023. *Financial Control In Public Sector As A Measure For Preventing Fraud And Fund Misuse*. Linkedin.com. https://www.linkedin.com/pulse/financial-control-public-sector-measure-preventing-fraud-chibuike#:~:text=Internal%20controls%20are%20a%20critical%20component%20of
47. Carcello, J.V. and Nagy, A.L., 2004. Audit firm tenure and fraudulent financial reporting. Auditing: a journal of practice & theory, 23(2), pp.55-69.
48. Courtois, C. and Gendron, Y., 2020. The show must go on! Legitimization processes surrounding certified fraud examiners’ claim to expertise. *European Accounting Review*, *29*(3), pp.437-465.
49. Chen, X. and Metawa, N., 2020. Enterprise financial management information system based on cloud computing in a big data environment. *Journal of Intelligent & Fuzzy Systems*, *39*(4), pp.5223-5232.
50. Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M. and Imine, A., 2023. Credit card fraud detection in the era of disruptive technologies: A systematic review. *Journal of King Saud University-Computer and Information Sciences*, *35*(1), pp.145-174.

51. Choudhary, A., Choudhary, G., Pareek, K., Kunndra, C., Luthra, J. and Dragoni, N., 2022. Emerging cyber security challenges after COVID pandemic: a survey. *Journal of Internet Services and Information Security*, *12*(2), pp.21-50.
52. Copland, S. 2021. Fingerprint. https://fingerprint.com/blog/anti-fraud-technology-post-pandemic/
53. Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2013. Internal control-integrated framework. COSO.
54. Cressey, D. R. 1953. Other people's money: A study in the social psychology of embezzlement. Glencoe, IL: Free Press.
55. Dorminey, J., Fleming, A. S., Kranacher, M., & Riley, R. A. 2012. The evolution of fraud theory. Issues in Accounting Education, 27(2), 555-579.
56. Daraojimba, R. E., Farayola, O. A., Olatoye, F. O., Mhlongo, N., & Oke, T. T. 2023. Forensic accounting in the digital age: a US perspective: scrutinizing methods and challenges in digital financial fraud prevention. *Finance & Accounting Research Journal*, *5*(11), 342-360.
57. Darsono, D., Ratmono, D., Putri, E. R. P., Cahyonowati, N., & Lee, S. 2024. An empirical analysis of asset misappropriation fraud during the COVID-19 crisis. *Problems and Perspectives in Management*, *22*(3), 314.
58. Davis, M. V. 2019. *Strategies to prevent and detect occupational fraud in small retail businesses* (Doctoral dissertation, Walden University).
59. Dimitrijevic, D., Jovkovic, B. and Milutinovic, S., 2021. The scope and limitations of external audit in detecting frauds in company's operations. *Journal of Financial Crime*, *28*(3), pp.632-646.
60. Denman, D. E. 2019. 2018 report on occupational fraud: results and how companies can protect their assets. *Journal of Accounting and Finance*, *19*(4).
61. Dias, A. P. 2021. Risks and Fraud. In *Proceedings of the 2nd International Conference in Accounting and Finance Innovation* (p. 69). UA Editora–Universidade de Aveiro 1st edition–December 2021.
62. Elbagoury, M. 2023. *The Fraud Diamond Theory*. Www.linkedin.com. https://www.linkedin.com/pulse/fraud-triangle-mahmoud-elbagoury
63. Efijemue, O., Obunadike, C., Taiwo, E., Kizor, S., Olisah, S., Odooh, C. and Ejimofor, I., 2023. Cybersecurity strategies for safeguarding customers data and preventing financial fraud in the United States financial sectors. *International Journal of Soft Computing*, *14*(3), pp.10-5121.

64. Erbuğa, G.S., 2022. Anti-Fraud and Anti-Corruption Tools in the Struggle Against Fraudulent Acts in the Public Sector. *Muhasebe Enstitüsü Dergisi*, (67), pp.57-70.
65. Eze, S., 2021. An Exploration of Internal Control Deficiencies and their Impact on Fraud in Local Churches in Nigeria.
66. Ehigie Aimienrovbiye Humphrey, Enofe A. O. and Ehigie Isoken Praise 2024 "Fraud Diamond: Detecting Fraudulent Behaviours in a Firm", *Journal of Corporate Governance Research*, 7(1). doi: 10.5296/jcgr.v7i1.20405.
67. Fish, G.P., 2020. Improving Accountants' Ability to Identify, Manage, and Prevent Fraud in Not-for-Profit Organizations.
68. Griffiths, M.D., 2010. Crime and gambling: a brief overview of gambling fraud on the Internet. Internet journal of criminology.
69. Goel, R.K., 2020. Medical professionals and health care fraud: Do they aid or check abuse?. *Managerial and Decision Economics, 41*(4), pp.520-528.
70. Galbraith, D., Tallapally, P. and Mondal, S., 2024. THE PERVASIVE NATURE OF FRAUD: A STUDY OF ORGANIZATIONS FROM PRE to POST PANDEMIC. *Co-Editors*, *3*, p.73.
71. Goldberg, L.M., 2012. *Greed, fear and irrational exuberance-the deep play of financial and cultural speculation* (Doctoral dissertation, UNSW Sydney).
72. Grant Thornton. 2021. *The next normal: Preparing for a post-Pandemic fraud landscape*. Retrieved September 24, 2024, from https://www.grantthornton.com/content/dam/grantthornton/website/assets/content-page-files/advisory/pdfs/2021/next-normal-preparing-post-pandemic-fraud-landscape.pdf
73. Griffin, C. C. 2017. *The Challenges of Combating Healthcare Fraud* (Master's thesis, Utica College).
74. Gunasegaran, M., Basiruddin, R., Abdul Rasid, S. Z., & Mohd Rizal, A. 2018. The case studies of fraud prevention mechanisms in the Malaysian medium enterprises. *Journal of Financial Crime*, *25*(4), 1024-1038.
75. HAKAMI, T.A. and Rahmat, M.M., 2019. Fraud Prevention Strategies: The Perception of Saudi Arabian Banks Employees. *Asian Journal of Accounting & Governance*, *11*.
76. Hilal, W., Gadsden, S.A. and Yawney, J., 2022. Financial fraud: a review of anomaly detection techniques and recent advances. *Expert systems With applications*, *193*, p.116429.

77. Hamza, M., Tehsin, S., Humayun, M., Almufareh, M.F. and Alfayad, M., 2022. A comprehensive review of face morph generation and detection of fraudulent identities. *Applied Sciences*, *12*(24), p.12545.

78. Hameed, S., Khan, F.I. and Hameed, B., 2019. Understanding security requirements and challenges in Internet of Things (IoT): A review. *Journal of Computer Networks and Communications*, *2019*(1), p.9629381.

79. Halder, R., 2022. Treasury Management and Working Capital Management of Akij Cement Company Limited.

80. Holtfreter, K. 2015. Financial fraud: Understanding and preventing financial crime. Springer.

81. Hassan, S. W. U., Kiran, S., Gul, S., Khatatbeh, I. N., & Zainab, B. 2023. The perception of accountants/auditors on the role of corporate governance and information technology in fraud detection and prevention. *Journal of Financial Reporting and Accounting*.

82. Huber, D., & Scheytt, T. 2019. Fraud and accounting scandals: A systematic literature review. International Journal of Accounting Information Systems, 35, 100420.

83. Institute of Internal Auditors (IIA). 2021. The three lines model: An update of the three lines of defense. IIA.

84. Ibrahim, H., 2022. A Review on the Mechanism Mitigating and Eliminating Internet Crimes using Modern Technologies: Mitigating Internet crimes using modern technologies. *Wasit Journal of Computer and Mathematics Science*, *1*(3), pp.50-68.

85. Iriqat, I. and Yehya, K.R., 2020. The Role of the Public Policy Network in Making and Implementing Anti-Corruption Policies in Palestine. *Rev. Eur. Stud.*, *12*, p.1.

86. Ilmiha, J., & Suboh, A. S. 2024. The Effectiveness of Internal Control in Preventing Accounting Fraud in Financial Companies. *East Asian Journal of Multidisciplinary Research*, *3*(6), 2181-2192.

87. Kramer, L. 2015. Fraud risk management: Developing an integrated fraud risk framework. Journal of Business Fraud, 8(4), 23-45.

88. Kalovya, O.Z., 2023. Determinants of occupational fraud losses: offenders, victims and insights from fraud theory. *Journal of financial crime*, *30*(2), pp.361-376.

89. Kandel, B., 2020. Qualitative Versus Quantitative Research. Journal of Product Innovation Management, 32(5), p.658.

90. Kassem, R. and Turksen, U., 2021. Role of public auditors in fraud detection: A critical review. *Contemporary Issues in Public Sector Accounting and Auditing*, *105*, pp.33-56.

91. Khatri, K.K., 2020. Research paradigm: A philosophy of educational research. International Journal of English Literature and Social Sciences (IJELS), 5(5).

92. Kirongo, A. and Odoyo, C., 2020. Research philosophy design and methodologies: A systematic review of research paradigms in information technology.

93. KPMG. 2020. Global fraud survey. KPMG.

94. Krause, J. 2017. Financial fraud in the digital age: Prevention strategies. Journal of Financial Crime, 24(3), 382-396.

95. Khaksar, J., Salehi, M. and Lari DashtBayaz, M., 2022. The relationship between auditor characteristics and fraud detection. *Journal of Facilities Management*, *20*(1), pp.79-101.

96. Khando, K., Gao, S., Islam, S.M. and Salman, A., 2021. Enhancing employee's information security awareness in private and public organisations: A systematic literature review. *Computers & security*, *106*, p.102267.

97. Karpoff, J.M., 2021. The future of financial fraud. *Journal of Corporate Finance*, *66*, p.101694.

98. Kennedy, J.P., Rorie, M. and Benson, M.L., 2021. COVID-19 frauds: An exploratory study of victimization during a global crisis. *Criminology & Public Policy*, *20*(3), pp.493-543.

99. Kenyon, W. and Tilton, P.D., 2012. Potential red flags and fraud detection techniques. *A guide to forensic accounting investigation*, pp.231-269.

100. Kerwin, K.R. and Bastian, N.D., 2021. Stacked generalizations in imbalanced fraud data sets using resampling methods. *The Journal of Defense Modeling and Simulation*, *18*(3), pp.175-192.

101. Kaur, B., Sood, K. and Grima, S., 2023. A systematic review on forensic accounting and its contribution towards fraud detection and prevention. *Journal of Financial Regulation and Compliance*, *31*(1), pp.60-95.

102. Kranacher, M.J. and Riley, R., 2019. *Forensic accounting and fraud examination*. John Wiley & Sons.

103. Kaaria, A.G., 2022. *Human Resource Information Systems, Top Management Commitment and Organizational Performance of Commercial State Corporations In Kenya* (Doctoral dissertation, JKUAT-COHRED).

104. Koerniawati, D., 2021. The Remote and Agile Auditing: a Fraud Prevention Effort To Navigate the Audit Process in the Covid-19 Pandemic. *Jurnal Riset Akuntansi Dan Bisnis Airlangga*, *6*(2), pp.1131-1149.

105. Kember, D. and Corbett, M., 2018. and Produced. *Structuring the Thesis: Matching Method, Paradigm, Theories and Findings*, p.15.

106. Klapper, L. and Miller, M., 2021. The impact of COVID-19 on digital financial inclusion. *World Bank Report, 2021*.

107. Kankpang, K. 2018. EFFECT OF FRAUD SCHEMES ON THE OPERATIONAL COST OF MANUFACTURING FIRMS. *COMPARATIVE STUDY ON THE EFFECTS OF TAX AUDIT ON VALUE ADDED TAX (VAT) COMPLIANCE IN*, 189.

108. Kamensky, D. 2021. Globalization, COVID-19 pandemic and white collar crime: a new threatening combination. *The Lawyer Quarterly*, *11*(4).

109. Kamaliah, K., Marjuni, N. S., Mohamed, N., Mohd-Sanusi, Z., & Anugerah, R. 2018. Effectiveness of monitoring mechanisms and mitigation of fraud incidents in the public sector. *Administratie Si Management Public*, *30*, 82-95.

110. Kashona, S. 2019. *The effectiveness of internal control and internal audit in fraud detection and prevention: A case study of the Ministry of Finance-Namibia* (Doctoral dissertation, University of Namibia).

111. Kaur, B., Sood, K., & Grima, S. 2023. A systematic review on forensic accounting and its contribution towards fraud detection and prevention. *Journal of Financial Regulation and Compliance*, *31*(1), 60-95.

112. Lang, M., Connolly, L., Taylor, P. and Corner, P.J., 2023. The evolving menace of ransomware: A comparative analysis of pre-pandemic and mid-pandemic attacks. *Digital Threats: Research and Practice*, *4*(4), pp.1-22.

113. Levi, M. and Smith, R.G., 2022. Fraud and pandemics. *Journal of Financial Crime*, *29*(2), pp.413-432.

114. Levi, M., & Smith, R. G. 2021. *Fraud and its relationship to pandemics and economic crises: From Spanish flu to COVID-19*. Australian Institute of Criminology.

115.

116. Macailao, M. C. 2020. Raising the red flags: The concept and indicators of occupational fraud. *Journal of Critical Reviews*, *7*(11), 26-29.

117. Mariner, S. S. 2020. *The Relationship Between Occupational Fraud and the Number of Employees in Small Businesses* (Doctoral dissertation, Northcentral University).

118. Matagaro, D. K. 2018. *Factors influencing occupational fraud risk in supermarket chains in Kenya* (Doctoral dissertation, Strathmore University).

119. McCormack, C. A. 2022. *Strategies to Prevent Occupational Fraud in the Financial Sector* (Doctoral dissertation, Walden University).

120. Moore, J. 2016. *The relationship between organization size and occupational fraud*. Northcentral University.

121. Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. 2021. Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current psychiatry reports*, *23*, 1-9.

122. Maulidi, A. and Ansell, J., 2021. Tackling practical issues in fraud control: a practice-based study. *Journal of Financial Crime*, *28*(2), pp.493-512.

123. Ma, K.W.F. and McKinnon, T., 2021. COVID-19 and cyber fraud: Emerging threats during the pandemic. *Journal of Financial Crime*, *29*(2), pp.433-446.

124. Mohammadi, S., Saeidi, H. and Naghshbandi, N., 2020. Investigating the impact of board characteristics on money laundering: Evidence from Iranian listed companies. *Journal of Money Laundering Control*, *23*(4), pp.751-767.

125. Musyoki, K.M., 2023. Internal Control Systems and their role in Financial Fraud Prevention in Kenya. *African Journal of Commercial Studies*, *3*(3), pp.173-180.

126. MUKAH, S. T. 2020. Occupational fraud in micro-financial institutions in Cameroon: strategies for timely detection and control. *Journal of Economics and Management Sciences*, *3*(2), p1-p1.

127. Mansor, N. and Abdullahi, R., 2015. Fraud triangle theory and fraud diamond theory. Understanding the convergent and divergent for future research. *International Journal of Academic Research in Accounting, Finance and Management Science*, *1*(4), pp.38-45.

128. Mardiana, S., 2020. Modifying Research Onion for Information Systems Research. Solid State Technology, 63(4), pp.5304-5313.

129. Mouamer, F.M.A., Amuna, Y.M.A., Khalil, M.K. and Aqel, A., 2020. Impact of applying fraud detection and prevention instruments in reducing occupational fraud: case study: Ministry of Health (MOH) in Gaza strip.

130. Mache, Z.C., 2023. Extent of use of mobile phone applications for rural development in some rural communities of Vhembe District.

131. Mehta, B.S. and Singh, B., 2024. *Technology and the Future of Work: Reshaping the Workplace*. Taylor & Francis.

132. Morales, J., Gendron, Y. and Guénin-Paracini, H., 2014. The construction of the risky individual and vigilant organization: A genealogy of the fraud triangle. Accounting, Organizations and Society, 39(3), pp.170-194.

133. Maulidi, A. and Ansell, J., 2022. Corruption as distinct crime: the need to reconceptualise internal control on controlling bureaucratic occupational fraud. *Journal of Financial Crime*, *29*(2), pp.680-700.

134. Muhaise, H., Ejiri, A. H., Muwanga-Zake, J. W. F., and Kareyo, M. 2020. The Research Philosophy Dilemma for Postgraduate Student Researchers. International Journal of Research and Scientific Innovation, 7(4), 2321-2705

135. Mwangi, S.W. and Ndegwa, J., 2020. The influence of fraud risk management on fraud occurrence in Kenyan listed companies. *International Journal of Finance & Banking Studies (2147-4486)*, *9*(4), pp.147-160.

136. Nur, S., 2020. Students' Perception toward the Use of Deductive and Inductive Approaches in Teaching English Grammar. TESOL International Journal, 15(1), pp.6-19.

137. Nakitende, M.G., Rafay, A. and Waseem, M., 2024. Frauds in business organizations: A comprehensive overview. Research Anthology on Business Law, Policy, and Social Responsibility, pp.848-865.

138. Naher, N., Hoque, R., Hassan, M.S., Balabanova, D., Adams, A.M. and Ahmed, S.M., 2020. The influence of corruption and governance in the delivery of frontline health care services in the public sector: a scoping review of current and future prospects in low and middle-income countries of south and south-east Asia. *BMC public health*, *20*, pp.1-16.

139. Nawawi, A., & Salin, A. S. A. P. 2018. Internal control and employees' occupational fraud on expenditure claims. *Journal of Financial Crime*, *25*(3), 891-906.

140. Nilsson, N. J., Rouse, W. B., & Serafeimidis, V. 2021. Retail fraud prevention: A multifaceted approach. Journal of Consumer Protection, 34(2), 97-105.

141. Obiora, F. C., Onuora, J. K. J., & Amodu, O. A. 2022. Forensic accounting services and its effect on fraud prevention in Health Care Firms in Nigeria. *World Journal of Finance and Investment Research*, *6*(1), 16-28.

142. Oladejo, M. T., & Jack, L. 2020. Fraud prevention and detection in a blockchain technology environment: challenges posed to forensic accountants. *International Journal of Economics and Accounting*, *9*(4), 315-335.

143. Omar, M., Nawawi, A., & Puteh Salin, A. S. A. 2016. The causes, impact and prevention of employee fraud: A case study of an automotive company. *Journal of Financial Crime*, *23*(4), 1012-1027.

144. Ogbomo, O.L., Ojiakor Ijeoma, P., Esenohor, E. and Laurretta, O., 2022. Fraud Schemes and Fraudulent Accountants Prosecution. *Sciences*, *12*(1), pp.1143-1169.

145. Ojolo, T.L., 2020. *A criminological investigation into the lived experiences of cybercrime perpetrators in southwest Nigeria* (Doctoral dissertation).

146. O'Neil, I., Ucbasaran, D. and York, J.G., 2022. The evolution of founder identity as an authenticity work process. *Journal of business venturing*, *37*(1), p.106031.Ortiz, A. 2018. Strategies to reduce Occupational Fraud in Small Restaurants.

147. Ortiz-García, A. 2022. Strategies to Reduce Occupational Fraud in Small Restaurants. *Global Disclosure of Economics and Business*, *11*(1), 1-18.

148. Pararas, K. 2023. *Fraud Triangle*. National Whistleblower Center. https://www.whistleblowers.org/fraud-triangle/#:~:text=According%20to%20Albrecht%2C%20the%20fraud

149. Peicheva, M. 2012. The Role of the Human Resource Department in Fraud Prevention. *Economic Alternatives*, *2*, 107-112.

150. Pagano, A., 2020. *Digital account opening fraud on demand deposit accounts: an assessment of available technology* (Master's thesis, Utica College).

151. Perry, C., 1998. A structured approach for presenting theses. Australasian marketing journal (AMJ), 6(1), pp.63-85.

152. Peiris, G.K.H. and Aruppala, W.D.N., 2021. A study on fraud prevention and detection Methods in Sri Lanka. *Kelaniya Journal of Management*, *10*(2), pp.37-56.

153. Pomerleau, P.L. and Lowery, D.L., 2020. Countering Cyber Threats to Financial Institutions. In *A Private and Public Partnership Approach to Critical Infrastructure Protection*. Springer.

154. Pulcine, C. J. (2024, August 15). *2024 ACFE Report to the Nations: Unmasking the Impact of COVID-19 on Occupational Fraud*. Withum. https://www.withum.com/resources/2024-acfe-report-to-the-nations-unmasking-the-impact-of-covid-19-on-occupational-fraud/

155. Peltier-Rivest, D., & Lanoue, P. 2015. Fraud prevention and detection in small businesses. Journal of Small Business and Enterprise Development, 22(1), 20-30.

156. Pope, K. R., & Lee, C. 2019. Corporate whistleblowing: How to strengthen internal fraud detection systems. Wiley.

157. PwC. 2021. Global economic crime and fraud survey. PricewaterhouseCoopers.

158. Quesenberry, K. 2016. Fraud risk management: Building a resilient organization. Wiley.

159. Rashid, M.A., Al-Mamun, A., Roudaki, H. and Yasser, Q.R., 2022. An overview of corporate fraud and its prevention approach. *Australasian Accounting, Business and Finance Journal, 16*(1), pp.101-118.

160. Rane, J., Kaya, O., Mallick, S.K. and Rane, N.L., 2024. Influence of digitalization on business and management: A review on artificial intelligence, blockchain, big data analytics, cloud computing, and internet of things. *Generative Artificial Intelligence in Agriculture, Education, and Business*, pp.1-26.

161. Rubio, M.S., 2023. *FRAUD DETECTION BY ANALY-ZING HUMAN BEHAVIOR APPLY MACHINE LEARNING TECHNIQUES* (Doctoral dissertation, ESCUELA POLITÉCNICA NACIONAL).

162. Rybalchenko, L., Ryzhkov, E. and Ciobanu, G., 2022. Global consequences of the loss of business in countries around the world caused by fraud.

163. Ramadhan, M. S. 2022. Can forensic and investigation audit and whistleblowing detect fraud during the Covid-19 pandemic?. *Journal of Contemporary Accounting*, 116-137.

164. Rezaee, Z., & Riley, R. 2019. Financial statement fraud: Prevention and detection. Wiley.

165. Ryman-Tubb, N. F., Krause, P. J., & Garn, W. 2018. Fraud detection and prevention in the financial services industry. Journal of Financial Regulation and Compliance, 26(2), 110-130.

166. Rezaee, Z., & Riley, R. 2019. Financial statement fraud: Prevention and detection. Wiley.

167. Rustiarini, N. W., Nurkholis, N., & Andayani, W. 2019. Why do people commit public procurement fraud? The fraud diamond view. *Journal of Public Procurement, 19*(4), 345–362.

168. Stapleton, A.H., 2022. *The Financial Fraud Epidemic and How It Has Changed Business Fraud* (Master's thesis, Utica University).

169. Shoetan, P.O. and Familoni, B.T., 2024. Transforming fintech fraud detection with advanced artificial intelligence algorithms. *Finance & Accounting Research Journal*, *6*(4), pp.602-625.

170. Shonhadji, N. and Maulidi, A., 2021. The roles of whistleblowing system and fraud awareness as financial statement fraud deterrent. *International Journal of Ethics and Systems*, *37*(3), pp.370-389.

171. Sharma, R., Mehta, K. and Sharma, P., 2024. Role of Artificial Intelligence and Machine Learning in Fraud Detection and Prevention. In *Risks and Challenges of AI-Driven Finance: Bias, Ethics, and Security* (pp. 90-120). IGI Global.

172. Sohel, A., Alam, M.A., Waliullah, M., Siddiki, A. and Uddin, M.M., 2024. Fraud Detection In Financial Transactions Through Data Science For Real-Time Monitoring And Prevention. *Academic Journal on Innovation, Engineering & Emerging Technology*, *1*(01), pp.91-107.

173. Singh, A., 2013. THE ECONOMIC AND FINANCIAL CRISIS OF. *The Handbook of the Political Economy of Financial Crises*, p.213.

174. Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.K.R. and Burnap, P., 2020. Impact and key challenges of insider threats on organizations and critical businesses. *Electronics*, *9*(9), p.1460.

175. Singh, P. 2020. The role of fraud awareness in promoting an anti-fraud culture to prevent occupational fraud within a professional services department at a higher education institution. (Doctoral dissertation).

176. Śmiałek-Liszczyńska, P., & Wojtkowiak, G. 2023. Employee Control and Occupational Fraud in Remote Work. *Humanities and Social Sciences*, *30*(4-part 1), 269-277.

177. Sari, D. N., Fakhruddin, I., Pramono, H., & Pratama, B. C. 2023. The role of sharia compliance, Islamic corporate governance and company size in preventing internal fraud. Jurnal Ekonomi, 12(01), 335-344.

178. Sari, S. P. 2021. Hexagon fraud detection of regional government financial statements as a fraud prevention in the pandemic crisis era. *Wacana Journal of Social and Humanity Studies*, *24*(2).

179. Shepherd, D., & Button, M. 2019. Organizational inhibitions to addressing occupational fraud: A theory of differential rationalization. *Deviant Behavior*, *40*(8), 971-991.

180. Schuchter, A., & Levi, M. 2016. The fraud triangle revisited. Security Journal, 29(2), 107-121.

181. Singleton, T. W., & Singleton, A. J. 2011. Fraud auditing and forensic accounting. Wiley.

182. Smith, C. 2021. Post-pandemic fraud risk: Mitigation through technology. Journal of Risk and Control, 9(1), 45-62.

183. Skoczylas-Tworek, A. 2019. Proactive and Reactive Mechanisms for Fraud Prevention Based on the Example of WIG20 Companies. *Economic and Social Development: Book of Proceedings*, 136-146.

184. Shao, S. 2016. Best Practices for Internal Controls to Prevent Occupational Fraud in Small Businesses?

185. Śmiałek-Liszczyńska, P. 2023. On Reducing Occupational Fraud Risk in SMEs: Recommendations. *Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie, 999*(1), 79-90.

186. Sow, A. N. G., Basiruddin, R., Mohammad, J., & Rasid, S. Z. A. 2018. Fraud prevention in Malaysian small and medium enterprises (SMEs). *Journal of Financial Crime*, *25*(2), 499-517.

187. Suh, J. B. 2018. *Financial Industry Security: Managing Occupational Fraud Risk in South Korean Banking Institutions* (Doctoral dissertation, University of Portsmouth).

188. Suh, J. B., Nicolaides, R., & Trafford, R. 2019. The effects of reducing opportunity and fraud risk factors on the occurrence of occupational fraud in financial institutions. *International Journal of Law, Crime and Justice*, *56*, 79-88.

189. Suryanto, T. 2016. Dividend Policy, Information Technology, Accounting Reporting to Investor Reaction And Fraud Prevention. *International Journal of Economic Perspectives*, *10*(1).

190. Tepalagul, N., & Lin, L. 2015. Auditing standards and fraud detection in the manufacturing sector. Journal of Accounting and Economics, 56(1), 125-144.

191. Tunley, M., Button, M., Shepherd, D., & Blackbourn, D. 2018. Preventing occupational corruption: Utilizing situational crime prevention techniques and theory to enhance organizational resilience. *Security Journal, 31*(1), 21–52.

192. Torra-Prat, R., 2024. Vigilance and tax fraud in early modern Catalonia. *Social History, 49*(2), pp.117-142.

193. Thangavel, V., Global Identification of Smart Card Technologies-Safe and Secure: A Research.

194. Taherdoost, H., 2021. A review on risk management in information systems: Risk policy, control and fraud detection. *Electronics*, *10*(24), p.3065.

195. Taufik, T., 2019. The effect of internal control system implementation in realizing good governance and its impact on fraud prevention. *International Journal of Scientific and Technology Research*, *8*(9), pp.2159-2165.

196. Uddin, M.H., Ali, M.H. and Hassan, M.K., 2020. Cybersecurity hazards and financial system vulnerability: a synthesis of literature. *Risk Management*, *22*(4), pp.239-309.

197. Valiquette L'Heureux, A., 2022. The Case Study of Los Angeles City & County Fraud, Embezzlement and Corruption Safeguards during times of pandemic. *Public Organization Review*, *22*(3), pp.593-610.

198. Widiyati, D., Valdiansyah, R. H., Meidijati, M., & Hendra, H. 2021. The role of public accountants in fraud prevention and detection in the taxation sector during covid-19. *Golden Ratio of Auditing Research*, *1*(2), 73-85.

199. Wilasittha, A. A. 2022. The Remote Audit in Post-Pandemic Era: Professional Scepticism and Audit Quality Perspective. *Journal of Economics, Business, and Government Challenges*, *5*(02), 1-8.

200. Weidenhammer, E., Barger, J., & Harper, D. 2019. Retail fraud: Deterrence and detection. Journal of Retail Operations, 29(4), 212-225.

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

202. Wulanditya, P., Ardianto, H., & Sistiyarini, E. 2022. Relationship Among Ethical Value And Fraud Diamond In Banking Industry During Pandemic. *International Journal of Environmental, Sustainability, and Social Science*, *3*(2), 343-350.

203. Wells, J.T., 2017. *Corporate fraud handbook: Prevention and detection*. John Wiley & Sons.

204. Wen, S., Li, J., Huang, C. and Zhu, X., 2023. Extreme risk spillovers among traditional financial and FinTech institutions: A complex network perspective. *The Quarterly Review of Economics and Finance*, *88*, pp.190-202.

205. Whalley, B., France, D., Park, J., Mauchline, A. and Welsh, K., 2021. Towards flexible personalized learning and the future educational system in the fourth industrial revolution in the wake of Covid-19. *Higher Education Pedagogies*, *6*(1), pp.79-99.

206. Yange, T.S., 2019. A Fraud Detection System for Health Insurance in Nigeria. *Journal of Health Informatics in Africa*, *6*(2), pp.64-73.

207. Youvan, D.C., 2024. Anatomy of a Financial Collapse: The Role of Technical Glitches in Modern Financial Systems.

208. Zhu, X., Ao, X., Qin, Z., Chang, Y., Liu, Y., He, Q., & Li, J. 2021. Intelligent financial fraud detection practices in the post-pandemic era. *The Innovation*, *2*(4).

209. Zhang, W., Chen, J., & Yan, L. 2019. Employee training and occupational fraud: Evidence from a Chinese company. Asia-Pacific Journal of Accounting and Economics, 26(3), 234-253.

210. Zhao, J. L., Fan, S., & Yan, J. 2020. Overview of blockchain technology. Journal of Information Technology, 35(2), 108-121.

211. Zhu, X., Wang, Y., Chang, Y., Chen, R., & Li, J. 2024. Anti-Fraud Analysis during the COVID-19 Pandemic: A Global Perspective. *International Journal of Information Technology & Decision Making*, *23*(01), 37-55.

212. Zhang, Y., Wu, Q., Zhang, T. and Yang, L., 2022. Vulnerability and fraud: evidence from the COVID-19 pandemic. *Humanities and Social Sciences Communications*, *9*(1), pp.1-12.