Arab American University

Faculty of Graduate Studies

The Role of Internal Controls in Fraud Prevention and Detection: A Case Study of Domestic Banks in Palestine

By

Aseel Jamal Ahmad Alzaqlih

Supervisor

Dr. Firas Murrar

This thesis was submitted in partial fulfillment of the requirements for the Master`s degree in Fraud Protection

8 / 2025

Thesis Approval

"The Role of Internal Controls in Fraud Prevention and Detection: A Case Study of Domestic Banks in Palestine"

By

Aseel Alzaqlih

This thesis was defended successfully on 2/8/2025 and approved by:

Committee members	Signature
1. Dr. Firas Murrar: Supervisor	
2. Dr. Majeed Mansour: Internal Examiner	
3. Dr. Diama Abu Laban: External Examiner	

Declaration

I declare that the work in this study entitled “The Role of Internal Controls in Fraud Prevention and Detection: A Case Study of Domestic Banks in Palestine” was carried out by me under the supervision of Dr. Firas Murrar in the Department of Fraud protection. Also, I declare that the information in this study is the result of my own work, and it has not been presented before in another degree, diploma, or another university.

The Name of The Student: Aseel Jamal Ahmad Alzaqlih

ID: 202112537

Signature: Aseel Alzaqlih

Date: 17/10/2025

Dedication

To those whose prayers were the secret behind my success, and whose support lit the path before me...

To my great mother — the source of tenderness, the owner of a heart that never runs dry of love and prayer...

To my father — the pillar of my life and the source of my strength, who instilled in me determination and nurtured me with his wisdom...

To my beloved husband — my life companion and first supporter, who has been a home and a haven in every difficult moment...

To the flower of my life, the joy of my heart, whose presence within me was a driving force to overcome every challenge — my daughter and my beloved Watan...

To my siblings — those who shared life with all its ups and downs, and were always a source of strength and support...

And to the soul of my dear friend and colleague who left us in body but remains a kind and eternal memory in our hearts — I ask Allah to envelop you in His vast mercy.

I dedicate to you this fruit of my labor — in gratitude, love, and endless appreciation.

To all my family and friends,

I dedicate this work.

Acknowledgement

First and foremost, all praise and thanks to Allah, the Almighty, who granted me the strength and guidance to complete this thesis.

I extend my deepest gratitude, appreciation, and sincere thanks to my supervisor, Dr. Firas Morrar, for his continuous academic support and valuable guidance throughout the preparation of this thesis.
His insightful comments and thoughtful direction had a significant impact on shaping and refining this study, helping it reach its full potential.

My sincere thanks also go to Dr. Majeed Mansour and Dr. Diama Abu Laban for their time, valuable feedback, and constructive evaluation.

I would also like to express my appreciation to all my professors at the Department of Financial and Administrative Sciences at the Arab American University, from whom I have learned greatly and benefited from their knowledge and experience.

Lastly, my heartfelt thanks to everyone who contributed to the completion and final presentation of this work.

All praise is due to Allah, in the beginning and the end.

Abstract

This study aims to investigate the relationship between internal controls and fraud within Palestinian domestic banks. Its primary goal is to explore the reality of fraud cases, their causes, and the connection between robust internal controls and their efficacy in both preventing and detecting these crimes. This study is one of the few that specifically investigates the reality of fraud in Palestine.

To examine this cause-and-effect relationship, the research adopted a descriptive and causal design and mixed-methods approach (quantitative and qualitative). Data were collected from a sample of 67 employees selected through purposive (non-probability) sampling to ensure a demographically diverse population based on variables such as gender, age group, and educational level. A total of 67 questionnaires were distributed and all were returned valid, yielding a 100% response rate. The findings aim to provide valuable insights for Palestinian banks to strengthen their control environments and enhance their resilience against fraudulent activities.

This study results confirms that there is an increase of fraud cases within Palestinian local banks, driven primarily by a lack of customer security awareness, greed for quick profits, and the expanded reliance on electronic banking services. The research reveals a significant discrepancy between reported and actual fraud cases.

The study also highlights the impact of technological advancements and political-economic challenges, such as Gaza war. And reveals that Palestinian banks effectively use a comprehensive internal control system, including fraud risk assessments, customer awareness campaigns, and employee training, to prevent and detect fraud.

Additionally, the findings affirm a strong, negative relationship between robust internal controls and the propensity for fraud, highlighting that a multi-layered defense strategy is crucial. This strategy encompasses technological measures like two-factor authentication, continuous control monitoring, and advanced detection systems, which together form a resilient framework for safeguarding banking operations and mitigating the evolving threat of financial fraud.

Based on the study's conclusions the researcher suggested that banks need to enhance fraud prevention include developing comprehensive anti-fraud policies, establishing a dedicated specialized monitoring team, and implementing advanced AI-driven detection systems. Furthermore, strengthening both customer and employee awareness through targeted training, enhancing technological security measures like biometric authentication, and enforcing stricter operational controls such as transaction limits are essential. These integrated measures aim to create a robust, multi-layered defense system to significantly mitigate fraud risks.

Key word and phrases: Fraud, fraud detection, fraud prevention, internal controls, Palestinian local banks, fraud risk assessment.

Table of Contents

List of Tables

List of Figures

List of Appendices

List of Abbreviations

1.	ACFE	Association of Certified Fraud Examiners
2.	PMA	Palestine monetary authority
3.	FFU	Financial Follow-up Unit
4.	SPSS	Statistical Package for the Social Sciences
5.	FRA	Fraud Risk Assessment
6.	IIA	The Institute of Internal Auditors
7.	KYE	Know Your Employee
8.	COSO	The Committee of Sponsoring Organizations
9.	AICPA	American Institute of Certified Public Accountants
10.	PWC	PricewaterhouseCoopers
11.	AI	Artificial intelligence
12.	ML	Machine learning
13.	BCBS	The Basel Committee on Banking Supervision
14.	AML	Anti-Money Laundering
15.	CFT	Counter-Terrorism Financing

Chapter One
Introduction

Fraud continues to rise to new heights, affecting more businesses in more diversified ways than ever before (PricewaterhouseCoopers, 2020). It is inevitable that fraud will occur despite our best efforts to prevent and suppress it (Rahman & Anwar, 2014). According to the Association of Certified Fraud Examiners (ACFE) 2024 Report to the nations, firms incur an average loss of revenue per year of 5% due to fraud. Fraud happens when someone or institution in a position of confidence and accountability violates the rules on purpose for one's own or a company's advantage at the cost of the general interest. It is a global ailment that affects every organization and economy (Kolapo & Olaniyan, 2018). It is prevalent in both industrial and emerging countries, and its extent, causes, manifestation, and impact on institutional growth and performance vary by location (Inaya & Isito, 2016). Every organization faces the danger of fraud, which may be exterior or internal. Employees are the source of internal dangers, who could misuse their position to steal funds and other resources belonging to their employer for personal gain (Occupational fraud), on the other hand, external dangers are produced by contractors, customers, and government representatives who could try to get money unlawfully (Corporate Finance Institute, 2020).

Worldwide, the banking industry is essential to the advancement of any country's economy. One of the main worries for governments has always been banking industry’s frauds (Sood & Bhushan, 2020). Bank failure is primarily caused by massive frauds, which are exacerbated by a lack of controls or failure to adhere to existing rules, leading to suffering (Nyakarimi et al., 2020). Fraud charges have a detrimental impact on the financial results of the banking industry. To improve the performance of their finances, banks ought to constantly utilize the most recent, state-of-the-art hardware and software,

which will raise the likelihood of identifying, stopping, and maybe doing away with online bank fraud (Ogbeide, 2018).

An essential component of the banking industry is internal control, which serves to secure the company's resources and guarantee compliance with legislation and rules and improve the reliability and precision of financial reporting (Alisherovich & Ugli, 2023). Banks face competitive and changing market challenges, necessitating new approaches and monitoring duties, internal control is essential for successful management, as it helps businesses evaluate control components and make improvements (Alawaqleh, 2021). Internal control mechanisms ought to be user-friendly and suitable; staff members who follow internal controls should take rewards; Banks ought to switch up workers from time to time into positions that allow for such rotations to give employees a change of pace and find any situations where policy violations could have happened (Haddad, 2016). In the current financial environment, managing risk and the prevention of fraud in banks are crucial (Hassan, et al.,2023). It's critical to achieve equilibrium between consumers' and businesses' needs for privacy protection and fraud prevention (Găbudeanu et al., 2021).

In Palestine There are seven domestic banks regulated by Palestine monetary authority (PMA) (*BanksDirectory*, n.d.). Palestinian banks are prone fraud too, fraudsters targeted it many times before, internally and externally. According to Palestinian Central Bureau of Statistics 1434 fraud case reported in Palestine- west bank in 2022 in contrast with 1054 case in 2021 (Pcbs, 2023). Due to the increase in fraud cases Financial Follow-up Unit (FFU) in Palestine, recently published an awareness about fraud and its related financial losses (*Warning of Electronic Fraud*, 2018). PMA also issued many circulars about the fraud schemes that were recently widespread. For example, circular (05/2019) about copying bank cards in ATM and point of sale machines, circular (206/2020) about

social media fraud, and circular (105/2022) about inheritance trick. According to Anti-Money Laundering and terrorism financing Decree Law No. (39) of 2022, fraud is considered a predicate offence for money laundering in Palestine. Financially driven crimes, such as fraud, are clear precursors to money laundering (Gilmour, 2022). The banking industry system is essential to the money laundering activity because criminals want to be able to transfer enormous sums of money rapidly and effectively (Premti et al., 2021). Banking organizations with lax internal controls are vulnerable to money laundering. Internal control lapses, particularly those related to money laundering, have resulted in losses for a number of banks (Vijeyan & Rahmat, 2022).

1.1 The Research Problem

The increasing prevalence of fraud in financial institutions is a growing concern. Despite that the internal controls policies and procedures available, many banks are still exposed to fraud. During the period from 01/01/2023 to 30/06/2024, electronic fraud caused customer losses equivalent to $2,903,684 per (1,318) recorded case in Palestine. However, the actual reality may be higher as this number only represents reported cases by fraudulent customers to the bank. Some customers did not report being exposed to fraud or did not disclose the value of stolen money, and some cases did not have any financial impact (“Patterns of Electronic Fraud,” 2024).

The problem of this study is “what’s the relation of internal controls and avoiding & identifying fraud”, as we need to know to what extent we have effective internal controls regarding fraud, and if internal controls help the banks in fraud avoiding and identifying.

1.2 Objectives of the Study

This study aims to:

1. Identify fraud, internal controls, and Palestinian domestic banks.
2. Find that to what extent fraud crimes are increased in banks.
3. Find out to what extent banks have effective internal controls regarding fraud.
4. To discover the connection among internal controls and fraud prevention.
5. To discover the connection among internal controls and fraud detection.

1.3 Research Questions and Hypothesis

Questions

- In this study, the questions are:

Q1: What is Fraud, internal controls and Palestinian domestic banks.

Q2: Is there any increase in fraud crimes in banks.

Q3: Does banks have effective internal controls regarding fraud

Q4: Is there any connection among internal controls and fraud prevention.

Q5: Is there any relation among internal controls and fraud detection.

Hypotheses

- In this study, the hypotheses are;

H1: Fraud crimes are not increased in banks.

H2: Banks doesn’t have effective internal controls regarding fraud

H3: There is no connection among internal controls and fraud prevention.

H4: There is no connection among internal controls and fraud detection.

1.4 Significance of the study

Fraud is impacting more organizations than at any time before in a variety of ways as it continues to soar to greater levels. Palestinian domestic banks experienced fraud cases in many ways in the recent five years. As technology develops and new electronic tools appear, fraud methods and schemes evolve. Despite that we find lack in research about Palestinian banks, that has shed lights on those cases or tried to study the reasons, results, ways and motives of fraud.

According to the Association of Certified Fraud Examiners (ACFE) 2024 Report to the nations, firms incur an average loss of revenue per year of $3.1 billion due to fraud. and based on a sample study, FFU collected 549 complaints of suspected money laundering crimes between 2015 and 2018. These reports involved a variety of predicate crimes, including tax offenses, dealing in illicit drugs, bribery, stealing and burglary, fraud, and violations of trust (Murrar, 2021b). PMA circular (136/2022) about schemes of ML, fraud stated as the 4th predicated crime in Palestine for ML. Which shows the importance of researching this issue and knowing its causes.

On the other hand, this research may help banks in Palestine to review their internal controls, policies, and procedures to find out the gabs that led to fraud cases. This can lead to reduce fraud cases in banks and its losses and protect the bank's customers and their data.

1.5 Research Methodology

Research design

This study established a cause-and-effect relationship using a descriptive and causal data, and it is conducted for domestic banks in Palestine.

Data collection

Two resources will be used in this study. The primary resource consists of a survey spread to employees of assurance services in Palestinian local banks, and high-levels in regulatory authorities, because it is an effective method for collecting quantitative data. And interviews for collecting qualitative data.

The responses to the survey will be gathered via the web and a questionnaire will be created and sent using the respondents' emails, together with a cover sheet explaining the goal of the research, data on the researcher for future inquiries, and the participants' rights. Hard copy questionnaires will be offered to participants who do not choose to complete the survey via the internet and wish to obtain their consent more quickly. Other sources include scientific papers, books, and internet research studies since they serve as an alternative in the research review and feature earlier studies and theories employed in other masters and theses.

Data analysis

The SPSS program will be used to analyze the descriptive data since it has quantitative replies, as it delivers correct and visual illustrations, as well as effective and beneficial data analysis outcomes. Several tests, such as the correlation test and hypothesis test, are used in the SPSS program to evaluate inferential statistics, such as the relationship between variables and to examine research topics and hypotheses. To decide if fraud crimes are increased in banks, descriptive statistics (Frequency, mean, standard deviation, level of significance) will be used to examine the data. Results will be regarded as significant for p-value below 0.05. Every data analysis project has some limitations, such as data quality, size of sample, assumptions, methodology, along with its interpretation. These limitations can affect the validity, dependability, and capacity for generalization of

the findings. To address this limitation, it is proposed to implement data cleaning and validation techniques as a preliminary step. Additionally, employing data augmentation methods and leveraging external datasets can enhance the completeness and accuracy of the dataset. bootstrapping, and resampling approaches allow for more robust inferences even with limited data, providing a more accurate representation of the population.

1.6 Research Tools: Study area, sample size.

Population and sampling

This study will be in Palestine. The participants in this study are Palestinian local banks employees who works in assurance services departments, and high-level employees in regulatory authorities, which are approximately 100 employees. Based on the population we calculated our sample size which is 67 employees. A purposive sampling that is nonprobability sample is going to be used. I chose local banks as a population since they abide by Palestinian regulation. While foreign banks abide by the Palestinian regulations and the regulation of their country of origin. In addition, I gained expertise in their fields of work by working at two local banks, which made it simpler for me to contact them when I needed further information.

1.7 Literature Review

Fraud in banks

Fraud in banks is a complicated topic, making it challenging to comprehend its seriousness. The financial loss has a significant negative effect on the economy in addition to harming the goodwill of the specific bank concerned. The foundation of the banking sector is honesty and trust, and when those are compromised, there may be serious consequences. The failure of banks to recoup the funds that were lost to frauds and the ineffectiveness of apprehending the offenders was the worst blow those nations had to deal with (Paul et al.,2023). Over the last 50 years, even advanced markets and

long-functioning banking institutions have experienced substantial financial collapse and economic crises due to the growing size of frauds (Bhasin, 2015). The protection and safety of money placed in banks by individuals and businesses is the responsibility and liability of banking institutions. These deposits suggest that banks and customers are often the focus of fraud (Cuccia, 2023).

The global finance sector, particularly banking, is nowadays overshadowed by criminal activities conducted by both internal and external actors that distort information in order to generate profits (fraud) (Utami et al., 2020). Technological developments, financial pressure, and criminal cunning are viewed as the primary causes of the marked increase in fraud inside the banking industry (Yego, 2016). There seems to be a negative correlation between online fraud and banks' economic growth; the higher the level of fraud, the worse the bank performs (Cavaliere et al., 2021).

Internal controls in banks

The requirement for a reliable financial system has led banks to prioritize their own internal control performance (Koutoupis & Malisiovas, 2021). All corporate organizations need internal control, but the banking industry needs it more than any other because of the risks inherent in its operations that need to be reduced for optimal growth and earnings. Banks with superior financial results were those that successfully adopted internal control features (Asiligwa & Rennox, 2017). An atmosphere of integrity (personal), management's obligation to assess fraud risk (via internal control), and audit committee oversight (internal audit) are the three components of fraud avoiding and discovery (Sudirman et al., 2021).

The avoidance of fraud benefits from internal control. The more internal control an organization has, the more effectively fraud is prevented within the organization (Setyaningsih & Nengzih, 2020). Fraud is never an easy problem to solve. Implementing internal control will potentially lessen management collaboration about fraud. A successful internal control framework strives to guarantee that organizational operations are fast and successful (Handoyo & Bayunitri, 2021).

The relationship among internal controls and fraud prevention

Fraud prevention is the elimination of possibilities to commit fraud through building and carrying out of risk management (particularly fraud risk management) and internal controls (Roemkenya Madolidi Handoyo & Indah Bayunitri, 2021). The successful deployment of an internal control system is extremely beneficial in preventing and complicating fraud. This is due to monitoring inside the internal control system comprises strong control and softer control, both of which are used to avoid fraud (Taufik,2019).

The most important way to avoid fraud is to implement internal control systems into all organizational operations. Internal control has to be qualified in the creation of its monitoring structure and adhere to good standards in its execution in order to successfully stop fraud (Handoyo & Bayunitri, 2021). In terms of creating a favorable environment for the cohabitation of the administration and personnel, the control culture establishes the internal control rhythm of the business. A positive work environment is a key barrier against fraud by staff members (Wanjala & Riitho, 2020). Fraudulent conduct may be avoided in a company or group by stepping up participation and managerial oversight (Fernandhytia & Muslichah, 2020).

The relationship among internal controls and fraud detection

Fraud detection policy formulation is one of the many vital processes carried out through risk management to reduce risk factors, their weakness, and their influence (Taherdoost, 2021). Internal control should be developed in such way to be capable of meeting the needs of the organization in question. if the internal control is executed appropriately, it can be depended on to defend itself from fraud.

Policies ought to be established to guarantee that businesses, particularly banks, hire employees with the right skills for key roles and departments like internal audit. Moreover, companies such as banks have to implement a strategy that provides its audit personnel with up-to-date education regarding the latest audit trends. This will help the businesses discover and minimize fraudulent activity (Nwaobia, 2021). The stronger the internal control application, the more efficient fraud detection (Hadian et al., 2021). The internal control systems play an important role and is necessary for an auditor who is or will be involved in fraud detection (Gunawan et al., 2022).

1.8 Limitation of this study

In this study we found some limitations like:

- Lack of Palestinian literature about fraud.
- Lack of statistical information about fraud from official regulatory authorities.
- Lack of cooperation in answering questionnaires.
- Answers credibly to the questionnaires due to the sensitivity of the subject.

Chapter Two
General Framework
Introduction

This chapter lays forth the fundamental ideas required to comprehend fraud as a phenomenon and the methods intended to stop, identify, and evaluate it, especially in relation to the banking industry. The definition of fraud and an examination of its fundamental mechanics, such as the commonly recognized fraud triangle and the many types of fraud that occur in companies, are covered first.

Internal controls, which are the main line of defense against fraudulent activities, are then the topic of debate. The idea, significance, elements, and constraints of internal controls are discussed in this section, along with the several ways they could appear in real-world situations.

The chapter then explores fraud prevention and detection tactics, looking at the theoretical underpinnings as well as useful techniques that businesses may use to lower their risk of fraud. Additionally, the chapter presents Fraud Risk Assessment (FRA), a methodical procedure for assessing possible weaknesses in an organization and lists essential frameworks for carrying out FRA successfully.

Lastly, by concentrating on the banking industry in Palestine and providing insights into its structure and the unique fraud threats it confronts, the chapter puts these worldwide ideas into context. By bridging theoretical frameworks with practical issues, this localized examination lays the groundwork for more in-depth investigation in later chapters.

2.1 Fraud

2.1.1 **The concept of fraud**

We have several ways to define fraud. But first it is crucial to clarify where the term "fraud" could have come from. The expression "fraud" comes from the Latin word "fraus," which meaning illegal activity, injury, and dishonesty (Vassiljev & Alver, 2016).

Wells (2014) defined fraud as “any crime for gain that uses deception as its principal modus operandi.”. In Miriam-Webster’s Dictionary of Law (1996) fraud is defined as “any act, expression, omission, or concealment calculated to deceive another to his or her disadvantage.” (Greenlee et al., 2007). The ACFE stated that Any behavior that depends on lying to get an advantage is considered "fraud." If there is a "knowing distortion of the facts or hiding of an important fact order to convince someone to take action to his or her detriment," according to Black's Law Dictionary. Stated differently, lying to deprive someone or a company of their funds or assets is fraud.

The Bureau of Justice Statistics define fraud as acts that “intentionally and knowingly deceive the victim by misrepresenting, concealing, or omitting facts about promised goods, services, or other benefits and consequences that are nonexistent, unnecessary, never intended to be provided, or deliberately distorted for the purpose of monetary gain.” (Morgan, 2021). The Institute of Internal Auditors defines fraud as IIA (2019) "any illegal act characterized by deceit, concealment, or violation of trust".

We can notice that all definitions mentioned above share a common factor which is using deception to fool others. Which make them all suitable for our study, but the researcher will adopt wells’ definition of fraud for the study.

Deception is a component of scams, but not all deceit is a fraud. A fraud occurs when four conditions are met: significant fabrication, being aware of the false declaration, the target's dependence on the false claim, and the target's losses due to relying on the misleading declaration (Wells, 2014).

2.1.2 **Fraud triangle**

The Fraud Triangle is a framework that clarifies the variables contributing to fraudulent conduct inside businesses. (Sabău, 2013). It comprises three key aspects are pressure, opportunity, and rationality. The Fraud Triangle Theory was created by Cressey in 1953 and is based on three elements that lead to fraud convictions. Data of the fraud prisoners' hearings was gathered to create the framework. in the US. It was concluded that pressure, chance, and rationalization were the three basic components of fraud. He described pressure as a person's economic hardship that results in dishonesty as a means of relieving the financial strain that they have concealed from others. Another crucial component of fraud is opportunity. Possessing an advantage gives one the opportunity to perpetrate fraud without coming to light. It takes talents and familiarity with the present methods of operation for fraudsters to allow fraud by exploiting any discovered weaknesses. Rationalization is a final essential component of fraud. It is a personalized explanation triggered by a person's way. An inaccurate rationale will persuade invaders to assume that lying or concealing information is appropriate. Cressey proposed that for fraudulent activity occur, when all three conditions have to be met at the same time (Awang et al., 2020).

Figure 1. The Fraud Triangle (Cressy 1953)

Source: adapted from Wells (2014)

Many theories emerged after Cressey's theory, some of them modifies the parts of the triangle like rationalization and personal integrity, and the others add some elements to it like capability. Kassem and Higson (2012) argues that to have a deeper understanding of the causes for fraud, it is vital to consider several fraud models.

2.1.3 **Fraud categories**

Regretfully, there are a plethora of categories into which fraud might fall. However, at its core, all forms of fraud can be personal or institutional. Let's examine a few of each's salient features (Association of Certified Fraud Examiners, n.d.).

- **Fraud inside a company**

This is also referred to as "job-related fraud," and it occurs when a management, leader, or staff member of a firm fools the company. Consider tax evasion, misleading the investors and stockholders.

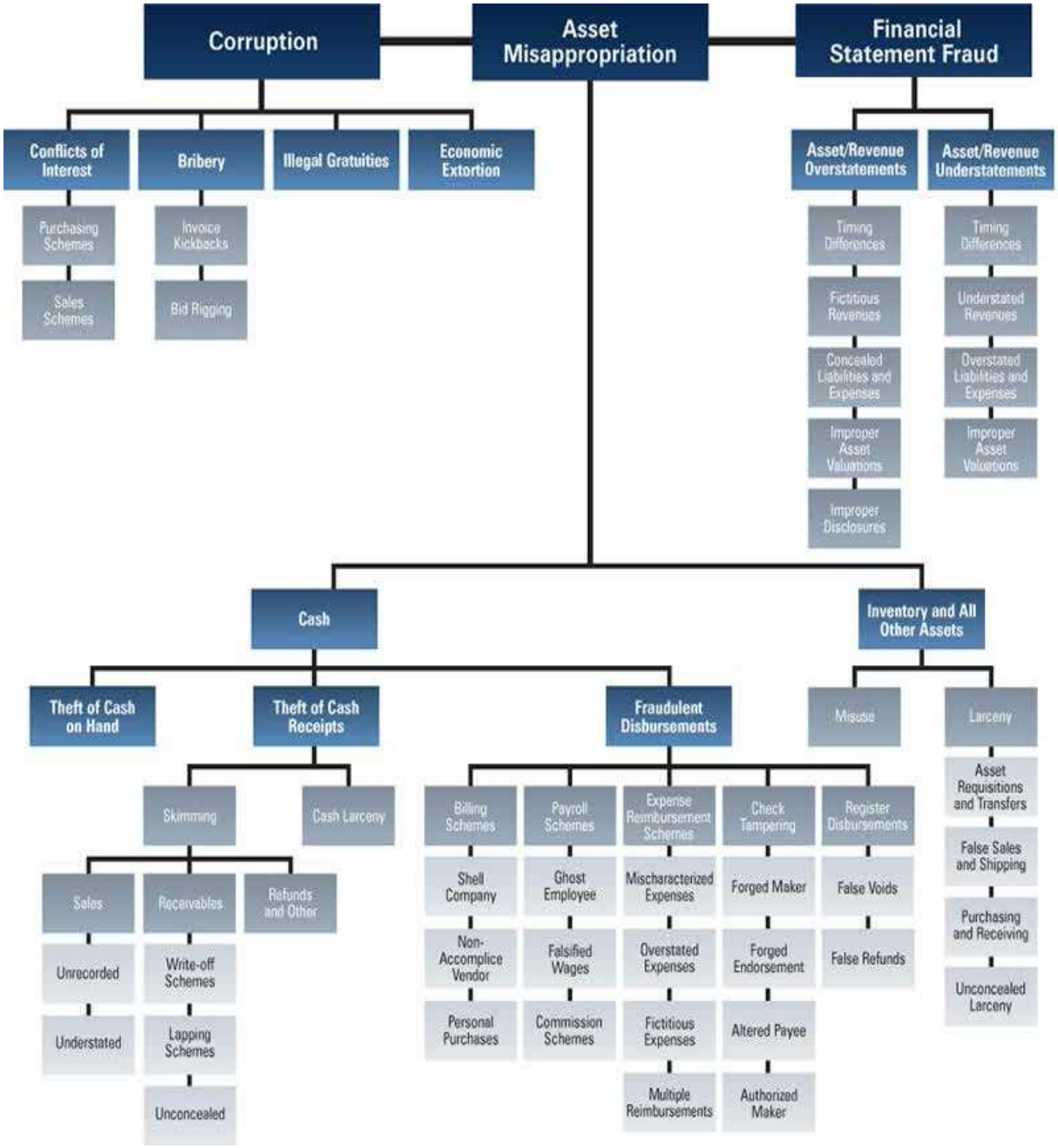

Figure 2. Occupational Fraud & Abuse Classification System (The Fraud Tree)

Source: Fraud 101: What is Fraud? (acfe.com)

Corruption, assets theft, and financial statement fraud are the primary types of occupational fraud. There is a distinct amount of incidence and median loss linked to every scheme. The most frequent type of fraud is asset misappropriation, whereas financial statement fraud is the most expensive for the companies, and the majority of

incidents that were declared encompassed corruption. As shown by the accompanying graphs.

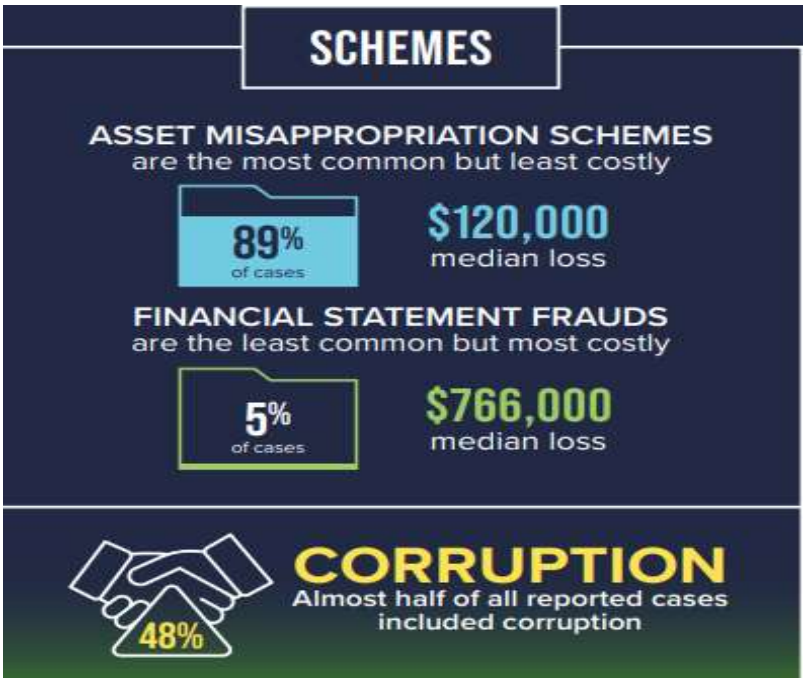

Figure 3. Fraud Schemes

Source: ACFE 2024 Report to the Nations

As occupational fraud affects each industry in society, it's critical to examine the variations among these industries. According to the data in (Figure 4), private firms are the ones where occupational fraud happens the most commonly. It is important to mention that these figures are based on an analysis of 1,1921 fraud instances, not an exhaustive list of every incident that have been reported. Nonetheless, they continue to offer a useful perspective on the realm of occupational fraud across several industries.

- **Against certain people**

The second category of fraud in which a criminal target just one individual using phishing, ID theft, and "advance-fee" schemes, among other tactics. The Ponzi scheme "which offers large profits to shareholders but takes fresh investors' funds to cover fees and give

previous shareholders substantial profits in the near term" is maybe among the most famous and destructive individual scams.

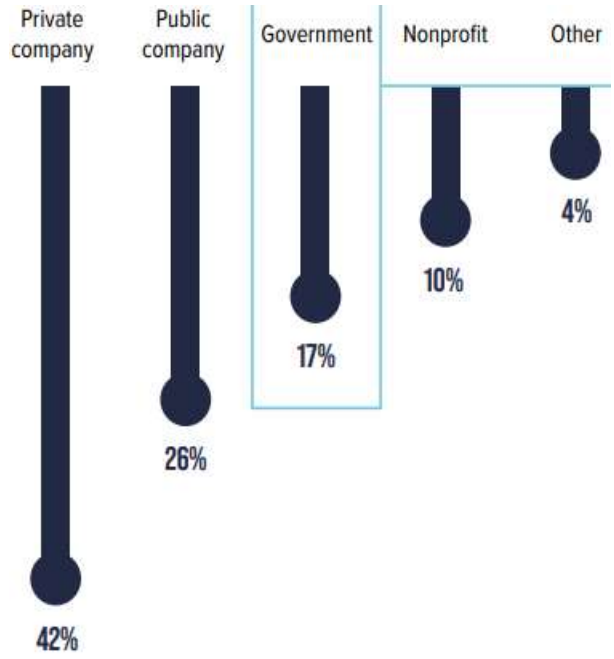

Figure 4. Kinds of companies that are prey to occupation-related fraud

Source: 2024-report-to-the-nations.pdf (acfe.com)

- **Fraud committed by outside groups.**

This covers external fraud affecting a business, such as contractors that fabricate what they do, request bribes from staff members, and manipulate expenses. However, there are instances in which consumers scam businesses— for instance, by attempting to return stolen or counterfeit products or by mailing fake cheques. Technology also poses a growing risk to businesses in terms of consumer data stealing and trademark theft.

For the straightforward reason that conducting business requires engaging with foreigners, external fraud poses a hazard for every firm. All businesses interact and communicate with clients, suppliers, outside experts, and anybody else who may access confidential information, affect corporate decisions, or exercise other forms of authority (Wells, 2014).

2.2 Internal Controls

2.2.1 The concept of internal controls

The Committee of Sponsoring Organizations' (COSO) defined internal control as a "process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance" (Internal Control | COSO, 2023).

Various concepts that describe the essence of internal control are embodied in the COSO framework:

1. Objectives: When properly designed and implemented, internal control is a structure that helps companies to accomplish their goals. Internal control ought not to be viewed as a collection of disjointed control processes since it is concentrated on achieving three types of goals (explained below).
2. Process: Internal control is a continuous procedure that all organizational levels carry out. It is not limited by a timeframe, roles, measurements, or collection of guidelines. Instead of treating internal control as a further burden upon top of whatever control processes they now follow, businesses should view it as a complete, optimized program.
3. People: Policies, procedures, and rules are not the focus of internal control. It all comes down to people: Individuals at every level of a company set goals and carry out actions intended to reach those goals.
4. Limitations: While internal control offers an acceptable level of certainty that the goals will be met, it is not a guarantee. Like all business activities, internal control systems are subject to failure. The applicability of an entity's goals, managerial

discretion, internal malfunctions, and outside happenings are all factors that can restrict the effectiveness of internal control programs.

5. Flexibility: The internal control framework is inherently adaptable. It may be used at all organizational levels, including the corporate level and the subsidiaries, branches, divisions, and departments. Internal control protocols should be modified by entities to meet the requirements of their hierarchical structure.

On the other hand, American Institute of Certified Public Accountants (AICPA) defined it as a process affected by organization's structure, work and authority flows, people, and management information systems, designed to help the organization accomplice specific goals or objectives (Compliance Supplement 2020, 2020).

Piskunov and Tarasova (2020) defined internal controls as an organization control system to ensure continuous functioning of accounting rules, execution of adopted programs and plans in accordance with the legislation.

In banks A framework of assurances and checks called internal control makes ensuring that a bank's activities follow rules, guidelines, and protocols. Ensuring that activities are conducted successfully, efficiently, and in accordance with regulations and standards is its primary goal. In addition, it encompasses implementing rules and processes to identify and stop mistakes, fraud, and misconduct. Examples of these procedures include confirming the correctness of financial transactions, separating responsibilities to avoid conflicts of interest, and making sure that all transactions have the necessary permissions and paperwork (Alisherovich & Ugli, 2023).

Al-Mashhadi (2021) defined internal control as a collection of tactics used inside an organization or divisions to confirm the implementation of monetary and managerial

regulations. It has evolved into an instrument used by administration to assess the efficacy of monitoring mechanisms and to give upper management the data they need to make choices about the operation of the division on both a monetary and managerial level.

The researcher will adopt that internal control is a system consisting of several tools formulated by the higher authorities of the organization to reduce the risks, ensure compliance with the instructions and laws in force, and to ensure the continuity of the institution's operations.

While, in this study internal control will be defined as recommended by COSO including the following categories:

- ✓ Dependability and correctness of financial documentation.
- ✓ Effectiveness as well as productivity of activities
- ✓ Adherence to relevant legal and regulatory requirements.

2.2.2 The importance of internal controls

A deficiency in internal controls or their circumvention account for Greater THAN 50% of professional fraud cases ("Occupational Fraud 2024: A Report to the Nations," 2024). Internal controls are getting more and more important due to globalization, expanding technological use, corporate hazards, and complicated company transactions (Otoo et al., 2023). Internal control has to be prioritized more, fraud inside a company is more likely to occur in those with inadequate internal control systems (Sudirman et al., 2021).

Enhanced operational efficiency and handling risks are two key benefits of using internal control. But in addition, it will assist management in the following (Bubilek, 2017):

1. The implementation of standardized protocols, guidelines, and directives.
2. Safeguarding the organization's present assets.

3. Delivering dependable financial statements.
4. Guaranteeing adherence to legal requirements.
5. Eradicating revenue or asset losses.
6. Precise and goal-driven decision-making.
7. Identifying and preventing fraudulent activities.

Internal control is generally very crucial for everything that is brought before decision-makers, particularly for making sure that activities are lawful and frequent and for enhancing the general level of data and supervisory performance (Da Silva Nogueira & Jorge, 2017).

Because banks are private, nobody truly understands the scope of internal control issues until a crisis occurs. In addition, useless boards of directors might have been misled into believing that internal controls are successful. Given how quickly the banking sector's economic model is evolving, this is additionally plausible (Ayagre et al., 2014).

Being aware of Basel 2 regulations is also necessary when trying to evaluate the effect of risk mitigation and internal control. This internal monitoring structure has five essential components that all banks in Palestine must adhere to.

1. The element of administrative oversight and control is additionally grounded in three fundamental tenets: the senior management's obligations, the board's duties, and the component's rigorous standards of integrity and ethical conduct.
2. Recognition and evaluation of risks.
3. Task segmentation and oversight of activities.
4. Communication and Data Technologies.
5. Remedial actions and imbalance adjustments (ibrabas).

The internal control framework of the bank is crucial to the equity evaluation procedure. When necessary, inside, or outside audits are involved in the capital evaluation process, in addition to an objective examination. The board of directors of the bank bears the task of guaranteeing that the management institutes a mechanism for evaluating the many risks, formulates a strategy to correlate risk with the bank's financial resources allocation, and implements a protocol for overseeing adherence to its own rules. The board should routinely assess if the internal control system in place is sufficient to guarantee the orderly and responsible execution of business (*Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version*, 2006).

Following an examination of the PMA programs and regulations, as well as the Basel 2 standards, the following key elements may be summed up for additional primary business review (Bayyoud & Sayyad, 2015):

- ✓ Check foreign exchange swings (between US dollars and Israeli shekels).
- ✓ Managing excessive levels of unpredictability.
- ✓ Effect of wider financial and political conditions on banking activities.
- ✓ Independence of internal control.
- ✓ Separation of responsibilities.
- ✓ Economic threat reveals crucial risk in the field.
- ✓ Basel 2 and global laws are aligned with bank plans.

In my opinion internal controls are foundational for the stability and integrity of banking operations, helping banks manage risks, comply with regulations, maintain financial accuracy, and protect assets. Creating internal control system starts from

implementing effective governance and accountable policy practices. The fundamental elements of an effective system are building an honest and ethical culture, as well as clearly communicating appropriate behavior and standards for each employee, analyzing the risks of fraud, establishing systems and procedures, and developing an appropriate oversight process.

2.2.3 **The components of internal controls**

Figure 5. The COSO Cube 2013

Source: KPMG. (2013). COSO Internal Control

Five elements make up COSO's definition of internal control which is control environment, risk evaluation, communication and data, control actions, and monitoring activities.

2.2.3.1 Control Environment

This establishes the tone for the company and affects employees' awareness of control. It serves as the basis for every other internal control element. Nuhaa et al., (2021) emphasized that the control environment relates to the mindset of administrators and

understanding of the company's internal control systems. It has an impact on strategic planning, targets, and systematic activity monitoring. It also outlines the setup technique and influences managerial awareness across staff. It acts as a base for subsequent components. Akinleye & Kolawole (2020) noted that the control environment refers to the behaviors, understanding, and acts of governance personnel about internal oversight and their duties in the institution. The control environment serves as a framework of successful internal control system implementation and operation.

2.2.3.2 Risk assessment

The practice of determining and assessing risks that are relevant to reaching objectives and providing information on how such risks ought to be handled. Organizations ought to apply fundamental guidelines for successful risk assessment.

- ✓ Accurately define goals to help identify and analyze risks connected to company goals.
- ✓ Evaluate risks to attain company goals and develop management strategies.
- ✓ Take into account possible fraud in the pursuit of goals.
- ✓ Determine and examine modifications that may affect internal control.

2.2.3.3 **Information and communication**

Systems and processes for information and communication that make it easier to identify, capture, and exchange data in a way and for a length of time that enables people to carry out their responsibilities. Accounting aims to enhance taking decisions through effective communication of data. Organizational problems and complexities can impair firms' capacity to take educated decisions, particularly when communication obstacles prevail.

Information and communication may significantly improve organizational effectiveness (Braim & Mohammed, 2023).

2.2.3.4 **Control activities**

Control activities are the rules and guidelines that guarantee administrative orders are followed. Frazer (2020) stated that the procedures and rules outline how directions from leadership will be implemented. Control operations include permissions, authorizations, confirmations, checks, operational performance assessments, asset protection, and separation of roles. These procedures prevent fraud and theft, reducing potential losses. COSO (2013) recognized three key elements for control activities:

- ✓ Design overall oversight actions to reduce the risk of reaching company goals to satisfactory levels.
- ✓ Manage technology to achieve company goals.
- ✓ Implement control actions based on established guidelines and processes.

2.2.3.5 Monitoring activities

procedures for assessing internal control functioning over a period in order to evaluate its level of effectiveness. Effective monitoring relies on every staff member understanding the organization's goals, mission, duties, and acceptable risk thresholds (Akinleye & Kolawole, 2020).

The efficacy of internal controls is favorably impacted by all five factors in the sequence of impact. Adopting a control system that is in line with the COSO guidelines and paying close attention to how its components are applied are necessary to improve functioning processes' productivity and effectiveness, boost the validity of accounting records, and

make sure that staff members abide by the relevant legislation and industry advancements (Abd et al., 2022).

Banks with better economic performance were those that effectively implemented internal management components. The regression analysis showed a substantial positive correlation among internal controls and the banking industry's financial results, with financial failures resulting from a scarcity of internal controls (Hanoon et al., 2021).

2.2.4 Internal controls limitations

The 2013 Guidelines addresses the limits of internal control. Companies are unable to constantly monitor occurrences or situations, and internal control systems may not always function as intended. Controls are carried out by individuals and are vulnerable to human mistake, errors in judgment, managerial overrule, and collusion (KPMG, 2013).

Organizations implement internal controls to guarantee that the accounting records are reliable and accurate. But these controls have limits, like the potential of collaboration, in which lower-level employees and supervisors allow operations without manager permission. Management overrides are also feasible because the practice cannot be stopped. Furthermore, these controls are intended to address routine transactions rather than uncommon ones, which might jeopardize the integrity of the business's accounting information if a large number of unexpected operations arise outside of normal oversight. Furthermore, human fault, such as employees doing routine errors during peak times or loss of staff is a concern (Team, 2023).

2.2.5 Forms of Internal Controls

Internal controls are characterized into three kinds, which will be addressed further below:

- ✓ Preventive controls are implemented to avoid fraud from happening in its initial place.
- ✓ Detective controls: Such controls are employed to detect fraud if it occurs regardless of the prevention measures in place.
- ✓ Corrective controls: They're the measures implemented once investigative controls find fraud.

2.3 Fraud Prevention

2.3.1 Concept of fraud prevention

Merriam-webster's definition of prevention is to keep something from happening or existing ("Prevent," 2025).

Fraud prevention refers to the method or collection of operations used to prevent, dissuade, identify, and handle fraudulent situations. The purpose of preventative measures is to limit the prevalence of fraud and its repercussions.

Prevention methods are frequently used as an element of a wider risk mitigation approach. Individuals and organizations may implement preventative steps. When properly executed, preventative methods can preserve companies' resources. Fraud prevention is a crucial aspect of keeping all sorts of companies safe and productive (Fraudcom International, 2024).

Hamid and Nasih (2021) defined prevention as an extremely cost-effective strategy to address financial imbalances caused by fraud. Organizations use several strategies to prevent and combat fraud. PWC defined it as effectively crafted and functionally efficient measures that safeguard a company from fraud of all types (PricewaterhouseCoopers, 2021).

ACFE defining fraud prevention as fighting fraud prior it happens and emphasized that it is critical to the sustainability of any firm. Companies should evaluate, implement, and enhance procedures for recognizing, avoiding, and preventing fraud prior it happens. The board members of shareholders, the auditing board, auditors from all levels, risk administration professionals, investigators, activities workers, and others must work together to control the danger of fraud (Association of Certified Fraud Examiners, n.d.).

The researcher will adopt that fraud prevention is the proactive work done to stop fraud from happening. It involves anticipating fraud or risks and implementing strategies to avoid or mitigate their impact.

2.3.2 Fraud prevention importance

Implementing a fraud protection plan assists in avoiding firms from failing, as fraud may have a significant impact on the firm results. Failing to identify and handle fraud risks can lead to significant losses and quick business demise. Fraud damages may harm a company's brand and shareholder confidence, regardless of it is able to recover.

Implementing a fraud prevention plan can save organizations revenue by reducing avoidable expenses. In today's competitive international atmosphere, wasting resources is unacceptable.

Fraud has grown into a common practice within organizations, rather than a rare event. Organizations that fail to defend themselves from fraud enhance their susceptibility and risk becoming victims. Implementing a fraud protection procedure builds confidence among shareholders, traders, directors, audit committees, executives, and community. Data from the fraud prevention procedure should not be skipped over. Correcting deficiencies in the fraud prevention workflow is crucial for identifying, disclosure, and correcting losses resulting from fraud (Tomaš & Todorović, 2016).

The company ought to put a fraud prevention and reaction plan implemented to effectively restrict and handle fraud incidents. Effective safeguarding measures, including a reaction plan, are crucial for preventing fraud (The Institute of Internal Auditors [IIA], 2019). The proverb "prevention is preferable than treatment,". Since it often takes a company longer to heal from fraud than it lost from the crime itself, it is extremely vital to prioritize tactics to avoid fraud from happening in the first time (ACFE, 2016).

2.3.3 Fraud prevention methods

Prevention tactics may include preventing prospective criminals, identifying illegal conduct, and handling fraud events (Tomaš & Todorović, 2016). Several strategies, consisting of routine operational checks, cash inspections, ethical officers, password security, and internal control assessment and enhancement, can be used to stop fraud. Internal auditors carry out operational checks to evaluate the utilization of resources and reduce fraud activities. Performance audits evaluate the auditee's efficient use of resources in achieving project goals. Internal control is put in place to guarantee integrity within participating officers. Since cash is a highly liquid asset and is particularly vulnerable to fraud, cash evaluations are essential to safeguarding it. Ethics inspectors ought to amend their guidelines of behavior to reflect the most recent advancements in technology and science (Zamzami et al., 2016).

Separation of roles, IT credentials and permissions controls, tangible asset controls, education and evaluation, and firewalls are examples of preventive measures in companies. The idea of division of obligations guarantees that an individual cannot misuse the system on their own. The least privilege concept ought to serve as the foundation of IT credentials and permission restrictions, allowing users to only have the minimal amount of access required for their jobs. employees ought to only receive

physical authority over assets if it is required for their work. Training and frequent testing should be provided to staff members to make sure jobs are completed exactly as written. The purpose of firewalls and backups is to shield the company from outside threats and minimize disastrous consequences in the event of an incident (Bwerinofa, 2023).

2.4 Fraud Detection

2.4.1 Concept of fraud detection

Checking operations as they happen and spotting unusual activity before it can do serious damage are key components of immediate fraud detection (Bello et al., 2023).

The process of determining if an activity is fraudulent is known as fraud detection. It entails examining customer habits and finding trends in data. Utilizing analysis of data, putting in place detection tools, and teaching staff members to spot fraudulent trends are all part of avoiding fraud. Companies can safeguard themselves against monetary losses and harm to their image by adopting proactive strategies. Because AI and machine learning can discover tendencies and abnormalities rapidly and effectively, they are being employed more and more for fraud detection (Fraudcom International, 2024).

The techniques and processes that, with the help of cutting-edge technology, continuously monitor for fraud in important risk segments (PricewaterhouseCoopers, 2021).

The researcher will adopt that fraud detection process refers to the systematic approach used to identify, investigate, and prevent fraudulent activities within various systems and contexts. It involves the implementation of strategies, technologies, and methodologies designed to recognize and address deceptive behaviors and transactions that could result in financial loss, reputational damage, or legal consequences.

2.4.2 Importance of fraud detection

Fraud detection is essential for several causes. Financial companies can avoid significant losses that could arise if fraud was discovered after the fact by spotting fraudulent activity right away. It contributes to preserving consumers' confidence in financial organizations by protecting their funds and private data. Strong fraud prevention procedures are mandated by regulatory obligations imposed on financial organizations. Organizations can abide by these rules with the aid of fraud detection. By reducing the resources required for fraud investigation and correction, fast fraud detection helps financial organizations run more effectively (Bello et al., 2023). For businesses to safeguard their financial resources, uphold client confidence, adhere to legal obligations, stop monetary crime, and reduce reputational threats, fraud detection is essential. It assists businesses in spotting and stopping fraud, averting large losses. Establishing a dedication to security and preserving relationships with consumers are further benefits of effective fraud detection. Adherence to regulatory mandates aids in evading fines and legal obligations. Businesses play a vital role in the fight against financial crime, which includes money laundering and the funding of terrorism, by identifying and stopping fraudulent activity. Maintaining the image of a business and its brand integrity is another benefit of effective fraud detection (Fraudcom International, 2024).

2.4.3 Fraud detection methods

Fraud detection methods, including synthetic intelligence, machine learning, information analysis, and process oversight and inspection, can help companies identify and stop fraudulent activity by analyzing intricate patterns and abnormalities in information, thereby enhancing their capability to identify and prevent fraudulent actions. To identify and stop fraud, financial organizations like banks use a mix of internal controls,

technology, and staff education. Banks can prevent fraud and safeguard the financial resources of their consumers by utilizing cutting-edge technologies and strategies (Financial Crime Academy, 2024).

A robust fraud detection program requires a combination of tools and strategies, including computer machine learning and intelligent technology (machine learning/artificial intelligence), machine identification, transaction fraud inspection, and behavioral analysis. Behavioral analytics monitors activity trends, while device fingerprinting tracks authorized users and detects changes in access patterns. ML/AI enhances these methods by analyzing data from numerous honest and fraudulent transactions (*Fraud Detection in Banking: 2024 Guide*, 2024).

2.5 Fraud Risk Assessment (FRA)

2.5.1 Concept of FRA

Risk assessment is an ongoing and continual procedure that identifies and analyzes risks to determine the way risks ought to be handled, to accomplish the goals of the organization. Management takes into account any modifications to the way it operates and outside circumstances that can make it harder for it to achieve its aims (KPMG, 2013).

The strategy for determining and evaluating risks to the entity's goals being met. It serves as the foundation for deciding how hazards will be handled (International Finance Corporation [IFC], 2021).

The practice of proactively detecting and mitigating a company's weaknesses to internal as well as outside fraud is known as fraud risk assessment. Since each business is unique, the process of assessing fraud risk is frequently more of an art than a science. It is important to customize the evaluation and assessment process to the specific needs of the company; there is no standardized method (Wells, 2014).

2.5.2 Importance of FRA

A business should be aware of the dangers that it faces, both directly and indirectly, to prevent fraud and in order to successfully safeguard its stakeholders. A systematic evaluation of the fraud risk, customized to the objectives, sector, size, and nature of the company, need to be carried out and evaluated on a regular basis (Rossi & Lietz, 2022).

Tools for risk assessment are essential to avoid fraud, and they ought to be improved to stop fraud in the financial industry. Frequent use of risk specialists can assist in spotting possible fraud indicators early on and averting actual fraud. Furthermore, it is important for firms to provide staff with frequent training on risk assessment methodologies in order to enhance their ability to identify and manage risks. By discouraging fraudsters before they perform their crimes, this training acts as a fundamental line of protection against them. Thus, fraud may be avoided, and a safer financial environment can be ensured by improving risk assessment processes and employing risk specialists in the banking industry (Nyakarimi et al., 2020).

A comprehensive risk assessment is necessary to determine the primary fraud risks, estimate their possible impact on the company, and implement crucial controls to detect and prevent fraud. (PricewaterhouseCoopers, 2021). Organizations looking to safeguard their interests, uphold stakeholder confidence, and negotiate the intricacies of today's business environment must adopt a proactive strategy to fraud risk evaluation. Companies may strengthen their defenses against threats, increase their resilience, and maintain long-term success by methodically detecting, evaluating, and managing fraud risks (Fraudcom International, 2024).

2.5.3 Who Conducts FRA

The executives and members of the board are in charge of controlling the risk of fraud. They should know, in particularly, how the company is handling increased risks and new exposures, as well as how the public and stakeholders are scrutinizing it; what kind of Fraud Risk Control Program the company has implemented; how it recognizes fraud risks; what steps it is taking to more effectively avoid fraud, or at least identify it earlier; and what procedures are in position to look into fraud while taking remedial action. Additionally, it is the duty of all employees, regardless of degree, to comprehend the consequences of fraud and the significance of stopping it (ACFE, 2016).

A fraud risk assessment can be carried out effectively by employees within the firm or by leveraging external resources. In either case, it is vital that the personnel leading and conducting the FRA remain impartial and independent throughout the process. Also, they must have a thorough understanding of the business (Wells, 2014).

2.5.4 The Framework for Seven-Step FRA

Financial Crime Academy (2024b) shows how to use the components of a risk of fraud evaluation in a thorough and organized manner:

- ✓ Identifying of possible schemes and inherent fraud risks.
- ✓ Evaluation of the probability of known intrinsic fraud hazards.
- ✓ Evaluation of the effects of known inherent fraud risks.
- ✓ An assessment of the individuals and divisions most likely to perpetrate fraud.
- ✓ Determining and connecting current controls to pertinent fraud risks.
- ✓ Assessment of the effectiveness and efficiency of the selected controls.

- ✓ Identifying, assessing, and taking appropriate action to reduce any remaining fraud risks.

2.5.5 A simple five-step for Evaluating the Risk of Fraud

There are five easy steps your business can take to reduce the risk of fraud, even if it may seem overwhelming. Determine risks, assess risks, manage risks, monitor and assess risks, and produce risk reports are the five steps (Vicente, 2023).

Figure 6. Steps to Conduct FRA

Source: What Is a Fraud Risk Assessment? And Why Do I Need One? | AuditBoard

Through interviews, surveys, and a risk evaluation matrix, hazards are identified and quantified as part of the FRA process. It puts mitigation efforts in order of priority and concentrates on dealing with major hazards first.

A plan is used to quantify and reduce risks, frequently in conjunction with risk experts and audit specialists. There are four ways to respond to risks: accepting, transferring, minimizing, and avoiding.

Risk assessment and monitoring are essential for preventing fraud. It is important to

define quantifiable actions, prescribe control efforts, and provide objective reporting. It's also critical to have precise documentation of the procedures and standards for alerting law enforcement.

2.6 Basel Committee Standards on Fraud Prevention Requirements

The Basel Committee on Banking Supervision (BCBS) provides international regulatory frameworks to enhance the stability and integrity of the banking sector. While Basel standards primarily focus on risk management, capital adequacy, and liquidity, they also address fraud prevention indirectly through principles related to operational risk, governance, and internal controls.

Key Basel Standards Relevant to Fraud Prevention

1. Basel II – Operational Risk Management (2004)

Basel II introduced Operational Risk as a key risk category, which includes fraud risk. Banks must allocate capital for operational risks, including:

- Internal Fraud (e.g., employee theft, misappropriation of assets)
- External Fraud (e.g., cybercrime, forgery, third-party scams)

Requirements:

- Banks must implement strong internal controls and fraud detection mechanisms.
- Three Lines of Defense Model:
    - First Line (Business Units): Fraud risk identification in daily operations.
    - Second Line (Risk & Compliance): Monitoring and enforcing anti-fraud policies.
    - Third Line (Internal Audit): Independent fraud risk assessments.

2. Basel III – Strengthening Governance & Controls (2010 onwards)

Bael III reinforced risk management requirements, indirectly impacting fraud prevention by emphasizing:

- Enhanced Corporate Governance: Banks must ensure board-level oversight of fraud risks.
- Stronger Internal Controls: Regular audits, segregation of duties, and fraud risk assessments.
- Transparency & Reporting: Timely reporting of fraud incidents to regulators.

3. Principles for Sound Management of Operational Risk (2011, Revised 2021)

The BCBS issued guidelines specifically targeting operational risk, including fraud:

- Risk Identification: Banks must proactively identify fraud risks (e.g., phishing, insider fraud).
- Risk Mitigation: Implement automated fraud detection systems (e.g., AI-based transaction monitoring).
- Incident Reporting: Maintain logs of fraud events and report material losses to regulators.

Fraud Prevention Measures Recommended by Basel

While Basel does not prescribe specific anti-fraud tools, it encourages banks to adopt best practices such as:

1. Know Your Employee (KYE) & Background Checks
    - Screening employees to prevent insider fraud.
    - Role-based access controls to limit unauthorized transactions.
2. Transaction Monitoring & AI-Based Fraud Detection

- Real-time alerts for suspicious transactions.
- Behavioral analytics to detect unusual customer/employee activity.

3. Cybersecurity & IT Controls
    - Strong authentication (e.g., multi-factor authentication).
    - Encryption of sensitive data to prevent breaches.
4. Whistleblowing Mechanisms
    - Secure channels for employees to report fraud anonymously.
5. Regulatory Reporting
    - Disclosing fraud-related losses in financial statements.
    - Complying with AML/CFT (Anti-Money Laundering/Counter-Terrorism Financing) rules, which overlap with fraud prevention.

Application in the Palestinian Banking Sector

Palestinian banks, supervised by the Palestinian Monetary Authority (PMA), are expected to align with Basel standards, particularly in:

- Strengthening internal fraud controls (e.g., preventing loan fraud, embezzlement).
- Enhancing digital security (e.g., protecting against cyber fraud in online banking).
- Improving governance to reduce fraud risks in high-risk areas like trade finance.

Challenges for Palestinian Banks:

- Limited resources for advanced fraud detection systems.
- Political instability increasing external fraud risks (e.g., hacking, financial crime). (Basel Committee on Banking Supervision [BCBS], 2017) (Basel II:

International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version, 2006).

2.7 Financial and Banking Sector in Palestine

The Palestinian financial sector plays a crucial role in sustaining economic activity despite the challenging political and economic conditions imposed by the Israeli occupation. The sector consists of banking institutions, insurance companies, microfinance organizations, and capital markets.

Due to restrictions on movement, trade, and access to resources, the Palestinian financial system faces unique challenges, including limited monetary sovereignty (as Palestine has no independent currency and relies on the Israeli shekel, US dollar, and Jordanian dinar) and dependence on correspondent banking relationships with international banks. Nevertheless, the sector has demonstrated resilience, with steady growth in banking penetration and financial inclusion efforts.

The Palestinian Monetary Authority (PMA) regulates banks in the West Bank and Gaza Strip, working to develop the financial sector and maintain monetary stability. The sector includes both local banks and branches of foreign banks. Major Palestinian banks like Bank of Palestine and Arab Bank serve a significant portion of the population. Some challenges are face the banks include limited access to international financial markets, restrictions due to Israeli occupation, and economic instability. The ongoing political conflict and economic restrictions impact banking operations, lending practices, and the overall stability of the financial system. There's been a push towards modernizing banking services, including mobile banking and fintech solutions, to adapt to the needs of the population. while the banking sector in Palestine is making strides, it continues to navigate complex challenges inherent to the region (“PMA Annual Report 2023,” 2024).

Key Features of Palestinian Banks:

Dual Currency System: Banks operate mainly in Israeli shekels (ILS), US dollars (USD), and Jordanian dinars (JOD), reflecting the economy's dependence on foreign currencies.

High Liquidity but Limited Lending: Due to economic instability, banks maintain high liquidity but are cautious in extending credit, leading to a low loans-to-deposits ratio compared to regional peers.

Strong Deposit Base: Palestinian banks rely heavily on customer deposits rather than interbank or international borrowing.

There are thirteen banks in Palestine, six foreign banks and seven local banks, figure 7 below shows banks with year of founding for local banks or opening the first branch for foreign banks, and the total number of branches and offices of representation.

Figure 7. Banks in Palestine
Source: Annual Report 2023.pdf (pma.ps)

According to PMA and FFU laws and instructions, every bank in Palestine must have four assurance departments, which is Internal Audit, Compliance, Risk and Anti-Money Laundering and Counter-Terrorism Financing departments. PMA Instructions No. 10 of 2017 that Related to rules and best practices for banks governance, and Anti-Money Laundering (AML) and Counter-Terrorism (CTF) Financing Decree Law No. (39) of 2022 and its amendments No. (45) of 2022 from FFU shows requirement, tasks and responsibilities for every department.

2.8 Risk of Fraud in Palestine

Based on the Association of Certified Fraud Examiners (ACFE) 2024 Report to the nations, fraud costs firms an average of 5% of their income each year. A large number of nations globally experienced tough conditions during the pandemic, which fraudsters took advantage of. According to the instances studied, fraudsters developed a variety of fraud schemes (Murrar, 2021a).

Based on a sample study, FFU collected 549 complaints of suspected money laundering crimes between 2015 and 2018. These reports involved a variety of predicate crimes, including tax offenses, dealing in illicit drugs, bribery, stealing and burglary, fraud, and violations of trust (Murrar, 2021b). PMA circular (136/2022) about schemes of ML, fraud stated as the 4th predicated crime in Palestine for ML.

War on Gaza have caused the number of fraud cases to rise, exacerbated by economic hardship and displacement. This has led to increase vulnerability, aid mismanagement, and cyber fraud. Reports of fraudulent claims for humanitarian aid have emerged, with some individuals or groups misrepresenting their needs to access resources meant for the most vulnerable. The rise in online activities has also led to a rise in cyber fraud, where scammers exploit the situation to deceive people. There have been allegations of

corruption within organizations responsible for distributing aid, leading to misallocation of funds. Fraud and corruption can erode public trust, complicating future recovery and aid efforts. Fraudsters lure victims with false aid promises, claiming they provide support, donations, and prizes. Victims provide private data, particularly bank information ("Patterns of Electronic Fraud," 2024).

During the period from 01/01/2023 to 30/06/2024, electronic fraud caused customer losses equivalent to $2,903,684 per (1,318) recorded case in Palestine. However, the actual reality may be higher as this number only represents reported cases by fraudulent customers to the bank. Some customers did not report being exposed to fraud or did not disclose the value of stolen money, and some cases did not have any financial impact ("Patterns of Electronic Fraud," 2024).

PMA, FFU, Banks and Association of Banks in Palestine makes efforts to sensitize all parties about widespread fraud patterns, through circulars like (52/2024) about fraud through emails and social media posts (*Cyber Fraud Awareness Campaign*, 2024).

Conclusion

This chapter demonstrates that fraud occurs when four conditions are met: significant fabrication, awareness of false claims, target dependence, and losses due to misleading claims, and it can be internal or external. The Fraud Triangle Theory, developed by Cressey in 1953, consists of pressure, chance, and rationalization. It identifies three key components for successful fraud.

By giving both financial and non-financial information legitimacy and authenticity, internal control improves the assurance process. It lowers audit fees, boosts openness, and boosts stakeholder confidence. Internal control should be embraced by auditors for both private and public businesses (Frazer, 2020).

To support their crucial responsibilities in preserving organizational integrity, fraud prevention and detection concepts and techniques exist. To find and control any fraud risks, we employ the idea and practice of Fraud Risk Assessment (FRA).

New reforms and risk management techniques have strengthened the banking industry in Palestine. Banks are lowering financial risk by identifying risks utilizing the Basel 2 framework and PMA guidelines. For these processes to function effectively, staff training is advised review (Bayyoud & Sayyad, 2015).

In Palestine war on Gaza has heightened fraud, aid mismanagement, and cyber fraud, posed vulnerability and eroded public trust, causing misallocation of funds and compromising recovery efforts.

Chapter Three
Methodology
Introduction

This chapter outlines the research methodology used to the role of internal controls in fraud prevention and detection: A case study of domestic banks in Palestine. It offers a full explanation of the research strategy and data gathering procedures, population and sample of study, and analytical procedures used to address the research questions or hypotheses presented in Chapter 1. The choice of methodology is justified in relation to the research objectives and the type of the data requested.

The aim of this chapter is to ensure transparency, reliability, and replicability of the study by providing a clear and comprehensive account of how the research was conducted. The chapter begins by describing the overall research design. It then details the specific methods used for sampling, data collection, and data analysis.

By articulating the research process in a structured and logical manner, this chapter serves as the foundation for interpreting the results presented in the study.

3.1 research design

An online survey was created and used to assess the conceptual framework's hypotheses, amongst a sample of employees of assurance services in Palestinian local banks. And interviews were made with supervisors in financial follow- up unit in Palestine. We then go into great depth on the sample, questionnaire design, measuring tools, and data collection procedure.

3.2 Data collection process

After examining the general and material on internal control and avoiding and identifying fraud in Palestine, an organized survey was developed and delivered to the employees of assurance services in Palestinian local banks which are 7 banks. Which were purposively

selected that is nonprobability sample. The study technique involved conducting an online survey via mail. And two interviews were made with supervisors in financial follow- up unit in Palestine. The findings gathered were qualitative and quantitative in nature. The response was gathered for 22 statements in questionnaires and 12 statements in interviews, prepared around the fraud and the impact of current internal control on fraud avoiding and detection in Palestinian local banks.

3.3 Population and sample of study

The study conducted in Palestine. The participants in this study were Palestinian local banks employees who works in assurance services departments, and high levels employees in regulatory authorities. I chose local banks as a population since they abide by Palestinian regulation. While foreign banks abide by the Palestinian regulations and the regulation of their country of origin. In addition, I gained expertise in their fields of work by working at two local banks, which made it simpler for me to contact them when I needed further information.

Following a three-week collecting period, we received 67 completed questionnaires as responses from assurance services employees in Palestinian local banks, and two interviews with supervisors in financial follow-up unit in Palestine.

3.4 Validity and Reliability of the Instrument

3.4.1 Validity of the Study

Validity refers to the extent to which a study accurately measures what it intends to measure. Since this research relies on Google Forms for data collection, the following aspects of validity were considered.

The content validity of a questionnaire is crucial, as it ensures it covers all relevant aspects of the construct being measured. The survey items were developed based on a thorough literature review and aligned with research objectives. Expert validation was

sought to ensure the questions accurately represent the study's focus, and a pilot test was conducted to refine ambiguous questions.

The survey's face validity is ensured through pre-testing with a few participants to confirm its clarity and relevance and maintaining a logical flow of questions to enhance respondent understanding.

3.4.2 Reliability of the Study

Reliability is crucial for maintaining consistency in measurement, and Cronbach's Alpha was utilized to verify the internal consistency of scaled questions. The table below shows the Cronbach's alpha coefficients for the study tool domains. For knowledge management, there are 26 items with a Cronbach's alpha of 0.923, indicating acceptable consistency.

Table 3.1 Cronbach's Alpha coefficient of consistency for the Tool

Field	No. of Items	Cronbach's Alpha	Result/Pass
Prevalence of fraud	5	0.856	Yes
Internal controls	8	0.951	Yes
Fraud prevention	8	0.862	Yes
Fraud detection	5	0.737	Yes
Overall	26	0.923	Yes

3.5 Statistical Analysis Methods

The researcher utilized various statistical techniques and functions to analyze the collected data to achieve the study's objectives, answer research questions, and evaluate the validity of established theories.

A mixed-method approach combining descriptive and analytical statistics was used. Descriptive statistics, including frequencies, percentages, arithmetic means, and graphical representations, were used. Pearson's correlation coefficient was calculated to explore the

strength and direction of relationships between variables. The non-parametric chi-square test was used to test the goodness of fit. Cronbach's alpha coefficient was used to measure the questionnaire's dependability instrument. Data cleaning, analysis, and hypothesis testing were conducted using IBM SPSS version 25.0 (SPSS Inc., Chicago, IL, USA).

Chapter Four
Data analysis and results
Introduction

This part presents a statistical analysis of the study "The Role of Internal Controls in Preventing and Detecting Fraud: A Case Study of Local Banks in Palestine." The findings of the study in relation to the study questions are presented in the first section of this chapter, while the findings of the study hypotheses as perceived by the study sample are presented in the second section.

4.1 Sample characteristics

The survey data collected by the researcher from the field were analyzed statistically, the descriptive results were as follows:

Table 4.1 shows the characteristics of the study sample, illustrating the demographics and professional backgrounds of the respondents. Gender: The sample consisted of 41 males (61.2%) and 26 females (38.8%).

Age group: 26 individuals were between 20 and 30 years old (38.8%), and 25 individuals were between 31 and 40 years old (37.3%). Older age groups were less represented, with 14 participants (20.9%) between 41 and 50 years old, while only two participants were over 50 (3.0%). The participants' age distribution points to a significant concentration in the younger and middle adult age groups, especially those in the 20–40 age range. This can reflect the target population's demographics or of younger people's greater accessibility or degree of participation. The underrepresentation of those over 50 can indicate possible obstacles to involvement, such a lack of interest, a lack of computer proficiency.

Educational level: Most participants held a bachelor's degree, with 58 (86.6%). Eight participants (11.9%) held higher educational qualifications. In terms of years of

experience, 3 participants (4.5%) had less than one year of experience, while 21 participants (31.3%) had between one and five years of experience. The largest group consisted of 23 participants (34.3%) with 6 to 10 years of experience, and 20 participants (29.9%) with more than 10 years of experience. Most participants have at least a bachelor's degree, indicating a highly educated population based on their educational background. This would suggest that professionals or those employed in knowledge-intensive industries make up most of the sample. The dataset is further enhanced by the job experience distribution, which balances experienced and early-career workers. Because it includes a range of viewpoints from people at various stages of their careers, this combination improves the findings' dependability.

The career levels among the participants showed a diverse distribution, with 13 managers (19.4%), 8 deputy managers (11.9%), 19 supervisors or department heads (28.4%), and 27 functional positions (40.3%). The career level distribution points to a sample that is well-balanced and includes viewpoints from different organizational hierarchy levels. The inclusion of management and supervisory personnel guarantees that strategic and leadership perspectives are also considered, while the robust representation of functional jobs offers insightful information about operational reality. This diversity improves the study's overall breadth and applicability, especially when evaluating organizational policies like internal control and fraud prevention.

As for the participating banks, the participants were distributed as follows: Bank of Palestine had the highest representation with 13 participants (19.4%), followed by the National Bank with 12 participants (17.9%), Palestine Islamic Bank (9 participants), Investment Bank (8), Arab Islamic Bank (8), Al-Quds Bank (11), and Safa Bank (6).

Table 4.1 Illustrates the Sample Characteristics of the Study

Variable		N	%
Gender:	Male	41	61.2%
	Female	26	38.8%
Age Group:	20-30	26	38.8%
	31-40	25	37.3%
	41-50	14	20.9%
	50+	2	3.0%
Educational Level:	Diploma	1	1.5%
	PA	58	86.6%
	Higher Edu.	8	11.9%
Number of Years of Experience in Regulatory Departments:	less than 1 year	3	4.5%
	1-5	21	31.3%
	6-10	23	34.3%
	10+	20	29.9%
Job Level:	Director	13	19.4%
	Deputy Director	8	11.9%
	Supervisor/Head of Department	19	28.4%
	Employee	27	40.3%
Bank Name:	Arab Islamic Bank	8	11.9%
	Palestine Islamic Bank	9	13.4%
	National Bank	12	17.9%
	Investment Bank	8	11.9%
	Bank of Jerusalem	11	16.4%
	Bank of Palestine	13	19.4%
	Safa Bank	6	9.0%
	Total	67	100.0%

4.2 Prevalence of fraud

The table 3.3 reveal that all 67 participants (100.0%) are aware of bank fraud cases. A significant majority, 58 participants (86.6%), believe that bank fraud has increased recently, while only 9 participants (13.4%) think it hasn't. Additionally, 44 participants (65.7%) feel that the fraud cases reported to banks by customers represent a small percentage of actual fraud cases.

Table 4.2 Illustrates the Number, Percent and Standard Deviation for the binary answers of the tool.

Item	No		Yes		
	N	%	N	%	SD
1. Have you ever heard of bank fraud cases?	0	0.0%	67	100.0%	0.0
2. Do you think that bank fraud has increased recently?	9	13.4%	58	86.6%	0.34
3. Fraud cases reported to banks by customers represent a very small percentage of actual fraud cases.	23	34.3%	44	65.7%	0.47

4.3 Descriptive results

The 5-point Likert response scale of Agreement was used for the answers which consists of five items ranging from ("Strongly disagree"=1 to “Strongly agree."=5).

The rating score was determined according to the arithmetic averages for each item by subtracting the upper limit from the lower limit equal to (4) grades, and then dividing the difference by (3), so the length of the category was (1.33). Accordingly, the averages for estimating the responses of the research sample members to the tool were as follows: (1 – 2.33) represents a low rating, (2.34 – 3.67) represents a moderate rating and (3.68 – 5.00) represents a high rating. The percentage of agreement was calculated by dividing the arithmetic mean by 5 and multiplying the result by 100.

The study participants consistently rated all items related to fraud, internal controls, and prevention/detection strategies as "High".

Table 4.3 presents participants' opinions on the questionnaire items that constitute the study areas. The table includes mean scores, standard deviations, percentages, and overall agreement scores for each area.

The mean scores for all items ranged from 4.30 to 4.64, indicating a high level of agreement among participants. The percentages ranged from 86.0% to 92.8%, with a "high" level of agreement. Standard deviations ranged from 0.50 to 0.81.

Regarding customer awareness, the highest mean score (4.64, 92.8%) was recorded for the statement "Banks conduct customer awareness campaigns regarding fraud." Regarding employee training, the statement "Training employees on controls related to fraud detection helps detect it more effectively" also received a very high mean score (4.60, 91.9%). Regarding the causes of fraud, items related to the causes of fraud, such as "lack of security awareness among bank customers" (4.52, 90.3%) and "the rise of organized crime and greed for money" (4.46, 89.3%), received high ratings. The effectiveness of internal controls also received high ratings. Statements related to the effectiveness of internal controls in prevention, detection, and correction received high ratings.

Regarding technical metrics, technical metrics such as "the use of two-factor authentication" (4.52, 90.4%) and "banks protect their systems and devices" (4.51, 90.1%) were highly rated.

Procedural metrics also received high ratings regarding procedural controls, such as "controlling access to data and financial systems" (4.49, 89.9%) and "investigating complaints and reports related to fraud" (4.54, 90.7%).

The least high relative means were: “Review financial transactions periodically” (4.31, 86.3%) and “Improve internal investigation procedures” (4.30, 86.0%) with a high degree of agreement.

In overall, the table demonstrates a strong consensus among respondents regarding the critical role of internal controls, customer education, and technical measures in preventing and detecting fraud within domestic banks in Palestine.

Table 4.3 Illustrates the Mean, Standard Deviation and Percent of the study Tool

Item	Mean	SD	%	Degree
4. Technological advancements, the expansion of the internet, and businesses' reliance on this technology have caused the number of fraud cases to rise.	4.42	0.70	88.4%	High
5. The ongoing war in Gaza and the population's need for aid have caused the number of fraud cases to rise.	4.37	0.81	87.5%	High
6. Lack of security awareness among bank customers has caused the number of fraud cases to rise.	4.52	0.56	90.3%	High
7. The rise in organized crime and the greed for money has caused the number of fraud cases to rise.	4.46	0.64	89.3%	High
8. The bank has controls in place to prevent and mitigate fraud.	4.48	0.59	89.6%	High
9. Control mechanisms are implemented to detect fraud cases when they occur.	4.40	0.58	88.1%	High
10. Corrective measures are taken to ensure that detected fraud cases do not recur and to correct deviations.	4.49	0.50	89.9%	High
11. The bank's senior management periodically reviews and evaluates the effectiveness of internal controls.	4.49	0.59	89.9%	High
12. Banks conduct customer awareness campaigns regarding fraud.	4.64	0.51	92.8%	High
13. Fraud risks are assessed periodically and continuously to identify, analyze, and manage these risks appropriately.	4.42	0.55	88.4%	High
14. Effective internal controls play a role in fraud prevention within the bank.	4.51	0.53	90.1%	High
15. Educating customers about fraud topics and common methods leads to reduce exposure to fraud.	4.58	0.55	91.6%	High
16. Using two-factor authentication to access data helps reduce the incidence of fraud.	4.52	0.70	90.4%	High
17. Banks protecting their systems and devices used to implement banking services reduces exposure to fraud.	4.51	0.64	90.1%	High
A. Controlling access to data and financial systems.	4.49	0.53	89.9%	High
B. Periodically reviewing financial transactions.	4.31	0.58	86.3%	High
C. Investigating complaints and reports related to fraud.	4.54	0.53	90.7%	High
D. Ensuring that policies and procedures are properly implemented.	4.48	0.56	89.6%	High
19. Effective internal controls enable the bank to detect fraud early.	4.39	0.63	87.8%	High
20. The bank's use of advanced technical systems (automated transaction monitoring systems) leads to fraud detection.	4.42	0.55	88.4%	High
21. Training employees on controls related to fraud detection helps detect it more effectively.	4.60	0.52	91.9%	High
A. Increasing coordination between different departments.	4.34	0.59	86.9%	High
B. Improving internal investigation procedures.	4.30	0.63	86.0%	High
C. Regularly reviewing and updating controls.	4.46	0.53	89.3%	High

Table 4.4 presents participants' opinions on the four fields of the study related to fraud in the banking sector. The table includes mean scores, standard deviations, percentages, and overall agreement scores for each field.

Regarding the prevalence of fraud, participants reported a mean score of 4.44 and a standard deviation of 0.46, indicating that 88.8% agree that fraud is a significant problem in the banking sector.

Regarding internal controls, the mean score was 4.49 and a lower standard deviation of 0.39, reflecting a high level of confidence (89.8%) in the efficiency of these measures in avoiding and mitigating fraud. Participants also rated fraud revention measures with a mean score of 4.42 and a standard deviation of 0.43.

The mean score for fraud detection was 4.44, with a standard deviation of 0.40, and 88.8% agreed on the effectiveness of fraud detection mechanisms.

Table 4.4 Illustrates the Mean, Standard Deviation and Percent of the study Fields

No.	Field	Mean	SD	%	Degree
1	Prevalence of fraud	4.44	0.46	88.8%	High
2	Internal controls	4.49	0.39	89.8%	High
3	Fraud prevention	4.42	0.43	88.4%	High
4	Fraud detection	4.44	0.40	88.8%	High

4.4 Testing Hypotheses

First Hypothesis - H0: Fraud crimes are not increased in banks at the level (α ≤0.05).

Based on a "Chi-Square Goodness-of-Fit Test: A Chi-Square goodness-of-fit test was conducted to determine if the observed frequencies of Prevalence of fraud significantly differed from the expected frequencies."

Table 4.5 Chi-Square Goodness-of-Fit Test (Prevalence of fraud)

	Observed N	Expected N	Residual	Chi-Square	Asymp. Sig.
Moderate	9	33.5	-24.5	35.836[a]	.000
High	58	33.5	24.5		
Total	67				

The Chi-Square goodness-of-fit test revealed a significant difference between the observed and expected frequencies ($\chi^2 = 35.5$, df = 2, p = 0.000), suggests that the result is statistically significant. This means there is strong evidence to reject the null hypothesis, which posits that there has been no increase in bank fraud.

Conclusion: Based on the above results, we reject H0 and accept the alternative hypothesis that bank fraud is increased in banks.

Second Hypothesis - H0: Banks doesn't have effective internal controls regarding fraud at the level (α ≤0.05)

Based on a "Chi-Square Goodness-of-Fit Test: A Chi-Square goodness-of-fit test was conducted to determine if the observed frequencies of Internal controls significantly differed from the expected frequencies."

Table 4.6 Chi-Square Goodness-of-Fit Test (Internal controls)

	Observed N	Expected N	Residual	Chi-Square	Asymp. Sig.
Moderate	1	33.5	-32.5	63.836[a]	.000
High	66	33.5	32.5		
Total	67				

The Chi-Square goodness-of-fit test revealed a significant difference between the observed and expected frequencies ($\chi^2 = 63.8$, df = 2, p = 0.000), suggests that the result is statistically significant. This means there is strong evidence to reject the null hypothesis, which assumes that banks' internal controls are low effective internal controls regarding fraud.

Conclusion: Based on the above results, we reject H0 and accept the alternative hypothesis that banks' internal controls are high effective internal controls regarding fraud.

Third Hypothesis – H0: There is no correlation among internal controls and fraud prevention at the level (α ≤0.05).

The results of the correlation analysis between internal controls and fraud prevention indicate a strong positive relationship.

Table 4.7 Pearson Correlation among internal controls and fraud prevention

Variable		Internal controls	Fraud prevention
Internal controls	Pearson Correlation	1	.718**
	Sig. (2-tailed)		0.000
Fraud prevention	Pearson Correlation	.718**	1
	Sig. (2-tailed)	0.000	0.000

The Pearson correlation coefficient was 0.718, with a significance level of 0.000. This means that the higher the internal controls assessment score, the more effective fraud prevention is.

Conclusion: Based on the above findings, it appears that there is a correlation among internal controls and fraud prevention.

Fourth Hypothesis – H0: There is no connection among internal controls and fraud detection at the level (α ≤0.05).

The results of the correlation analysis between internal controls and fraud detection indicate a strong positive relationship.

Table 4.8 Pearson Correlation among internal controls and fraud detection

Variable		Internal controls	Fraud detection
Internal controls	Pearson Correlation	1	.707**
	Sig. (2-tailed)		0.000
Fraud detection	Pearson Correlation	.707**	1
	Sig. (2-tailed)	0.000	

The Pearson correlation coefficient was 0.707, which is positive and strong relationship, with a significance level of 0.000. This means that the higher the internal controls assessment score, the more effective fraud detection is.

Conclusion: Based on the above results, we reject H0 and accept the alternative hypothesis that there is a correlation among internal controls and fraud detection.

4.5 Case Processing Summary

Table 4.9 Case Processing Summary (Listwise deletion based on all variables in the procedure)

		N	%
Cases	Valid	67	100.0
	Excluded[a]	0	.0
	Total	67	100.0

4.6 Interview Findings

Introduction and General Framework:

1. Head of Information and Analysis Department at the Financial Follow-up Unit / Head of Pattern and Strategic Analysis Unit at the Financial Follow-up Unit.
2. Fraud exists and is considered a primary crime in money laundering cases in Palestine.

Fraud Spread and Its Causes:

1. Fraud cases have increased recently.
2. The COVID-19 pandemic significantly contributed to the rise in fraud cases because customers relied more on banking applications due to lockdowns, leading to the development of new fraud techniques.
3. Political and economic conditions in Palestine have increased financial difficulties, pushing some individuals towards fraud to obtain financial aid.
4. The expansion of electronic banking services and customers' heavy reliance on them.
5. Lack of awareness about banking confidentiality and customers' greed for quick profits make them vulnerable to fraud by sharing their personal information with unknown sources or on untrusted websites.
6. Weaknesses in some financial control measures lead to financial losses due to fraud.

Common Types of Bank Fraud in Palestine:

1. Electronic fraud is currently the most widespread type of fraud.
2. Fraudsters deceive victims with fake promises of lottery winnings, financial grants from wealthy individuals, or fake business deals.

3. Fraudsters create fake bank pages and announce fake prizes to steal personal customer information.
4. Hacking bank accounts and applications, changing customer details, and transferring money to other accounts inside or outside Palestine.

Underreporting of Fraud Cases:

1. Some customers do not regularly check their accounts and may not notice fraud, especially elderly individuals.
2. Some victims report fraud cases to other authorities like the police or public prosecution instead of banks.
3. Some customers avoid reporting fraud out of embarrassment or fear of admitting they were deceived.
4. The actual number of fraud cases is higher than the reported cases.

Proposed Measures to Combat Fraud:

1. Enhancing banking security protocols and using advanced technology for fraud prevention.
2. Setting transaction limits for electronic banking applications and cards.
3. Strengthening customer identity verification before allowing any account modifications.
4. Developing and using advanced fraud detection software to identify all possible fraud scenarios.
5. Monitoring and immediately shutting down fraudulent pages once detected.
6. Raising customer awareness through social media campaigns and SMS alerts.
7. Training bank employees and establishing a specialized fraud prevention team to monitor banking system breaches and fraud indicators.

Need for Legislative and Regulatory Enhancements:

7. There is an urgent need to update laws to keep up with financial crimes, especially electronic fraud and cross-border crimes.
8. A specialized law for electronic fraud and digital evidence is necessary to help judges issue strict rulings against fraudsters.
9. Technology is a double-edged sword, and as its usage increases, stronger regulatory measures are needed, such as biometric authentication and artificial intelligence for fraud detection.
10. Establishing appropriate regulatory measures and continuously improving them, while ensuring collaboration between all banking departments, will help reduce and detect fraud cases early.
11. Due to the current situation and the limited access of some customers to physical bank branches, enhancing electronic banking services requires stricter regulatory controls, verification of customer identities, transaction limits, and monitoring of devices used for banking applications to prevent fraudulent activities.

Chapter Five
Discussion and Recommendations

This this study aims to explore the relationship of internal controls and fraud prevention and detection in Palestinian local banks. This section summarizes and discusses the findings of the study through answering the research questions and hypotheses.

5.1 Discussion of Results

The study revealed that most respondents to the questionnaire believes that fraud cases are increased in Palestinian local banks recently, this was reinforced by the answers of interviews too. This aligns with global fraud reports (ACFE, 2024), which indicate that firms incur an average annual revenue loss of 5% due to fraud. And FFU report ("Patterns of Electronic Fraud," 2024), which stated that during the period from 01/01/2023 to 30/06/2024, electronic fraud caused customer losses equivalent to $2,903,684 per (1,318) recorded case in Palestine.

The study found that fraud cases reported to banks by customers represent a very small percentage of actual fraud cases, because Some customers, particularly elderly individuals, may not regularly check their accounts, leading to potential fraud. Victims may report fraud cases to authorities like the police or public prosecution, while others avoid reporting due to embarrassment or fear of admitting deception. FFU report ("Patterns of Electronic Fraud," 2024) stated that the actual reality of fraud cases may be higher than numbers in the report as this number only represents reported cases by fraudulent customers to the bank. Some customers did not report being exposed to fraud or did not disclose the value of stolen money, and some cases did not have any financial impact.

The study also revealed that the most common causes of fraud cases is lack of security awareness among bank customers which caused the number of fraud cases to rise. And customers' greed for quick profits which make them vulnerable to fraud by sharing their personal information with unknown sources or on untrusted websites. Skula et al. (2020) stated that the person, whether an employee or a consumer, is usually the weakest link, especially if they are uneducated. As a result, it is critical to supplement the efforts with public awareness and education. Kamran et al. (2021) mentioned that Lack of awareness about banking confidentiality and greed for quick profits further exacerbate fraud issue.

Technological advancements, the expansion of the internet, and businesses' reliance on this technology have caused the number of fraud cases to rise according to study results. Amoh et al. (2020) stated that the expansion of electronic banking services and customers' heavy reliance on them make them vulnerable to fraud. Fraudsters use electronic banking devices such as ATMs and credit cards to steal money from customers’ accounts. Murrar (2021a) mentioned that the COVID-19 pandemic has led to a surge in fraud cases due to increased reliance on banking applications during lockdowns. Political and economic challenges in Palestine have pushed individuals towards fraud for financial aid, especially during the ongoing war in Gaza as shown in study results.

The study result demonstrated that Palestinian local banks implement a range of internal controls aimed at preventing and mitigating fraud. These controls are designed to ensure prompt detection of fraudulent activities and enable swift corrective measures to prevent recurrence. The respondents confirms that banks conduct customer awareness campaigns regarding fraud. To enhance public vigilance, banks—alongside the Association of Banks in Palestine—conduct customer awareness campaigns through multiple channels,

including physical branches, SMS notifications, and social media platforms. These efforts aim to educate customers about common fraud risks and preventive practices.

Senior management plays a pivotal role in reviewing the effectiveness of these internal control systems. This finding aligns with the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which emphasizes that executive leadership is responsible for establishing and overseeing internal control mechanisms.

Furthermore, the study found that banks routinely conduct Fraud Risk Assessments (FRA) to systematically identify, analyze, and manage fraud risks. AuditBoard (2021) confirmed that risk assessment and monitoring are essential for preventing fraud. These assessments are considered a cost-effective approach, especially when compared to the financial and reputational damage caused by fraud.

The study examined the relationship between internal controls and fraud prevention in Palestinian local banks. And found that effective internal controls play a critical role in fraud prevention within banks by identifying potential vulnerabilities and ensuring that appropriate safeguards are in place. Fernandhytia & Muslichah (2020) emphasize that the propensity for accounting fraud is negatively impacted by internal control. The outcome stems from the notion that a corporation or organization may avoid fraudulent behavior by boosting activity and managerial control.

Educating customers about fraud topics and common methods is the best way to reduce exposure to fraud in respondents' opinion. By informing clients about common fraud methods and prevention tips through awareness campaigns, banks empower customers to recognize and avoid fraudulent schemes. Technological measures such as two-factor authentication (2FA) further strengthen security by requiring an additional verification

step before accessing sensitive data or systems. Moreover, banks are actively enhancing the security of their systems and devices used in delivering banking services. This includes controlling access to financial systems and data, regularly reviewing financial transactions for unusual activity, investigating fraud-related complaints and reports, and ensuring that internal policies and procedures are effectively implemented. Together, these comprehensive efforts create a multi-layered defense against fraud and reinforce the integrity of banking operations. Kamran et al. (2021) stated that to reduce the risks of using electronic banking and to counter and mitigate fraud threats, financial institutions must implement a reliable and up-to-date security system with a focus on training and education, and customer awareness techniques must receive more attention.

The study also find that effective internal controls enable the bank to detect fraud early. Hassan et al. (2023) confirmed that internal controls also lessen the incidence of fraud. The study gives training employees on fraud-related controls the highest confirmation as it significantly strengthens the bank's detection capabilities. Nyakarimi et al. (2020) emphasized that it is important for firms to provide staff with frequent training on risk assessment methodologies in order to enhance their ability to identify and manage risks. By discouraging fraudsters before they perform their crimes, this training acts as a fundamental line of protection against them. Thus, fraud may be avoided, and a safer financial environment can be ensured by improving risk assessment processes and employing risk specialists in the banking industry.

Such training not only increases awareness but also fosters better coordination between different departments, ensuring a more unified and effective approach to identifying and responding to fraud.

This is best supported by regularly reviewing and updating these controls to ensure they remain robust and responsive to emerging risks. Gunawan et al. (2022) stated that the internal control systems play an important role and is necessary for an auditor who is or will be involved in fraud detection. In addition, the bank's adoption of advanced technical systems, such as automated transaction monitoring, enhances its ability to detect suspicious activity. These systems contribute to improving internal investigation procedures by providing timely alerts and data for thorough analysis.

5.2 Recommendations

In light of the study's conclusions, I recommend the following changes to help Palestinian local banks increase the efficacy of their internal control systems and fraud prevention and detection.

These recommendations are made to **Policies and procedures**

- ✓ Developing specific anti-fraud policies and procedures involves creating comprehensive guidelines that clearly define what constitutes fraudulent behavior, outline prevention measures, and establish reporting and response protocols.
- ✓ Once these policies are formulated, they must be effectively communicated and distributed to all employees across the bank through multiple channels such as training sessions, emails, and internal portals. It is essential to ensure that every employee not only receives these documents but also reads, understands, and acknowledges their responsibilities related to fraud prevention.
- ✓ This can be achieved through assessments, acknowledgments, or periodic refresher training. Furthermore, strict enforcement mechanisms should be put

in place to guarantee compliance, including monitoring adherence, conducting audits, and implementing disciplinary actions for violations. This comprehensive approach ensures that the bank maintains a strong culture of vigilance and accountability, significantly reducing the risk of fraud.

- **Hiring a dedicated team**
  - ✓ Hiring a dedicated, specialized, and well-trained team responsible for continuously monitoring fraud cases within the bank. This team will conduct thorough analyses of each incident to identify root causes and patterns, enabling them to develop effective strategies to prevent future occurrences.
  - ✓ Additionally, the team will collaborate closely with other departments to implement corrective measures and enhance overall fraud prevention frameworks, ensuring the bank's systems remain resilient against evolving fraud tactics.
- **Specialized fraud detection system**
  - ✓ Implementing a specialized fraud detection system that continuously monitors transactions and activities to identify suspicious patterns indicative of fraudulent behavior.
  - ✓ This system should include advanced analytical tools and machine learning algorithms to study and analyze detected fraud patterns in depth. Based on these insights, the system will enable the bank to take proactive and targeted measures to combat ongoing fraud attempts.
  - ✓ Furthermore, it will support updating prevention strategies and controls regularly to ensure that identified fraud schemes do not recur, thereby strengthening the overall security framework and minimizing financial losses.

- **Awareness and Training**
  - ✓ Strengthening customers awareness about fraudulent acts in banks, through launching awareness campaigns about fraudulent acts in banks and the new schemes through the media, social media and awareness campaigns to ensure that it reaches most of the customers.
  - ✓ Training employees to recognize and respond to fraud indicators.
- **Technological Enhancements**
  - ✓ Using security systems and anti-viruses, banks and customers should ensure that all the devices that used for electronic banking services are protected and safe.
  - ✓ Developing and deploying advanced fraud detection software.
  - ✓ Technology is a double-edged sword—as its use expands, stronger regulatory measures like biometric authentication and AI-based fraud detection are necessary.
- **Operational Controls**
  - ✓ Setting transaction limits for electronic banking and cards.
  - ✓ Strengthening customer identity verification procedures.
- **Integrated Regulatory Framework**
  - ✓ Establishing and continuously improving regulatory measures, along with interdepartmental coordination, enhances early fraud detection and prevention.
- **Enhanced Controls in Electronic Banking**
  - ✓ As more customers rely on online banking, especially with limited access to physical branches, stricter controls are needed—such as identity verification,

transaction limits, and device monitoring—to safeguard electronic banking services.

- **Identifying common patterns of fraud schemes**
  - ✓ Identifying common patterns of fraudulent behavior is a crucial step in combating financial fraud, as it allows banks and financial institutions to implement effective measures and continuously update systems to counter these patterns.
  - ✓ Ongoing development of detection capabilities also enables the identification of new and emerging fraud schemes.
  - ✓ Additionally, analyzing the methods used in fraud is essential for understanding the exploited vulnerabilities, which contributes to strengthening preventive measures and enhancing response mechanisms.

References

Abd, W. H., Kareem, A. D., & Jassim, E. E. (2022). The role of the modern COSO framework in evaluating the internal control system through the mediating role of the internal auditor:(Al-Muthanna State University as a model). *resmilitaris*, *12*(2), 4376-4391.

Akinleye, G. T., & Kolawole, A. D. (2020). Internal controls and performance of selected tertiary institutions in Ekiti state: A committee of sponsoring organisations (coso) framework approach. *International Journal of Financial Research*, *11*(1), 405-416.

Association of Certified Fraud Examiners. (n.d.). *Fraud 101: What is Fraud?* https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud

Association of Certified Fraud Examiners. (n.d.). *Fraud Prevention & Deterrence*. https://www.acfe.com/fraud-resources/fraud-prevention-and-deterrence

Association of Certified Fraud Examiners. (2016). *Fraud Risk Management Guide, 2nd Edition*. https://www.acfe.com/-/media/files/acfe/pdfs/fraud-risk-tools/coso-fraud-risk-management-guide-second-edition-executive-summary.pdf

Alawaqleh, Q. A. (2021). The Effect of Internal Control on Employee Performance of Small and Medium-Sized Enterprises in Jordan: The role of Accounting Information System. *Journal of Asian Finance, Economics and Business*, *8*(3), 855–863. https://doi.org/10.13106/jafeb.2021.vol8.no3.0855

Alisherovich, T. S., & Ugli, N. B. B. (2023). Internal Control in Banks. *EUROPEAN JOURNAL OF BUSINESS STARTUPS AND OPEN SOCIETY*, *3*(3), 34-39.

Al-Mashhadi, A. S. J. (2021). Review on Development of the Internal Control System. *Journal of Accounting Research, Business and Finance Management*, *2*(1), 12–20. https://matjournals.in/index.php/JARBFM/article/view/6422

Amoh, J. K., Awunyo-Vitor, D., & Ofori-Boateng, K. (2020). Customers' awareness and knowledge level of fraudulent acts in electronic banking in Ghana: evidence from a universal bank. *Journal of Financial Crime*, *28*(3), 870–882. https://doi.org/10.1108/jfc-08-2020-0161

Asiligwa, & Rennox, G. (2017). The effect of internal controls on the financial performance of commercial banks in Kenya. *IOSR Journal of Economics and Finance*, *08*(03), 92–105. https://doi.org/10.9790/5933-08030492105

Auditboard. *What is a fraud risk assessment? And why do i need one?* (2021, April 8). https://www.auditboard.com/blog/what-is-fraud-risk-assessment/

Awang, N., Hussin, N. S., Razali, F. A., & Talib, S. L. A. (2020). Fraud Triangle Theory: calling for new factors. *Insight Journal*, *7*(1), 54–64. https://doi.org/10.24191/ij.v7i1.62

Ayagre, P., Appiah-Gyamerah, I., & Nartey, J. (2014). The effectiveness of internal control systems of banks. the case of Ghanaian banks. *International Journal of Accounting and Financial Reporting*, *4*(2), 377. https://doi.org/10.5296/ijafr.v4i2.6432

BanksDirectory. (n.d.). www.pma.ps. https://www.pma.ps/ar/BanksDirectory

Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive version. (2006, June 30). https://www.bis.org/publ/bcbs128.htm

Basel Committee on Banking Supervision. (2017). *Basel III: Finalising post-crisis reforms*. Bank for International Settlements. https://www.bis.org/bcbs/publ/d424.htm

Bayyoud, M., Sayyad, N. (2015). The impact of internal control and risk management on banks in Palestine. *International Journal of Economics Finance and Management Sciences*, *3*(3), 156. https://doi.org/10.11648/j.ijefm.20150303.12

Bello, O. A., Ogundipe, A., Mohammed, D., Adebola, F., & Alonge, O. A. (2023). AI-Driven Approaches for real-time fraud detection in US financial transactions: challenges and opportunities. *European Journal of Computer Science and Information Technology*, *11*(6), 84-102.

Braim, S. J., & Mohammed, R. B. (2023). The (COSO) framework: Implications of Internal Control Components on the performance manufacturing companies. *Qalaai Zanist Journal*, *8*(1), 1203-1227.

Bubilek, O. (2017). *Importance of Internal Audit and Internal Control in an organization - Case Study*. https://www.theseus.fi/bitstream/10024/129916/1/Bubilek_Olga.pdf

Bwerinofa. R. (2023, August 1). Preventing fraud with internal controls: A refresher. *Journal of Accountancy*. https://www.journalofaccountancy.com/issues/2023/aug/preventing-fraud-with-internal-controls-a-refresher.html

Cavaliere, L. P. L., Subhash, N., Rao, P. V. D., Mittal, P., Koti, K., Chakravarthi, M. K., Duraipandian, R., Rajest, S. S., & Regin, R. (2021). The impact of internet fraud on financial performance of banks. *Turkish Online Journal of Qualitative Inquiry*, *12*(6), 8126–8158. https://tojqi.net/index.php/journal/article/view/3260

Compliance Supplement 2020. (2020). In *American Institute of Certified Public Accountants*. AICPA. https://us.aicpa.org/content/dam/aicpa/interestareas/governmentalauditquality/resources/singleaudit/uniformguidanceforfederalrewards/downloadabledocuments/2020-omb-comp-supp/2020cspart6.pdf

Committee of Sponsoring Organizations of the Treadway Commission. (2013). Internal control-integrated framework. New York, NY.

Corporate Finance Institute. (2020, September 15). *Fraud Red Flags*. https://corporatefinanceinstitute.com/resources/knowledge/other/fraud-red-flags/#:%7E:text=All%20organizations%20face%20fraud%20risk%2C%20which%20can%20either,misappropriating%20resources%20and%20assets%20owned%20by%20their%20employer.

Cuccia, J. (2023). Fraud in Banking: A Review of Fraud Scams, Effects, and Antifraud Techniques in the Banking Industry.

Cyber Fraud Awareness Campaign. (2018). Association of Banks. https://www.abp.ps/ar/Article/694/%D8%AD%D9%85%D9%84%D8%A9-%D8%A7%D9%84%D8%AA%D9%88%D8%B9%D9%8A%D8%A9-%D8%A8%D9%80%D8%A7%D9%84%D8%A7%D8%AD%D8%AA%D9%8A%D8%A7%D9%84-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A

Da Silva Nogueira, S. P., & Jorge, S. M. F. (2017). The perceived usefulness of financial information for decision making in Portuguese municipalities. *Journal of*

Applied Accounting Research, *18*(1), 116–136. https://doi.org/10.1108/jaar-05-2014-0052

Fernandhytia, F., & Muslichah, M. (2020). The effect of internal control, individual morality and ethical value on accounting fraud tendency. *Media Ekonomi Dan Manajemen*, *35*(1), 112. https://doi.org/10.24856/mem.v35i1.1343

Financial Crime Academy. (2024, May 13). Uncovering Fraud Techniques: Detection and Prevention Strategies. *Financial Crime Academy*. https://financialcrimeacademy.org/fraud-detection-methods/?gad_source=1&gclid=CjwKCAjwxY-3BhAuEiwAu7Y6s_Q03_9hPm-Gj2y5_BIyNpGfubZjNEXR59pWMTg4IxBiEl4n52PpCBoC7wAQAvD_BwE

Financial Crime Academy. (2024b, May 23). The 7 step Fraud Risk Assessment Framework. *Financial Crime Academy*. https://financialcrimeacademy.org/the-7-step-fraud-risk-assessment/

Fraud Detection in Banking: 2024 Guide. (n.d.). https://www.cosive.com/fraud-detection-in-banking-guide

Fraudcom International. (2024, May 2). *Fraud risk assessment – A proactive approach*. Fraud.com. https://www.fraud.com/post/fraud-risk-assessment

Fraudcom International. (2024, March 4). *What is fraud detection and why is it needed?* Fraud.com. https://www.fraud.com/post/fraud-detection

Fraudcom International. (2024, March 18). *What is fraud prevention and how does it help protect your business?* Fraud.com. https://www.fraud.com/post/fraud-prevention

Frazer, L. (2020). Does internal control improve the attestation function and by extension assurance services? A Practical Approach. *Journal of Accounting and Finance*, *20*(1).

Găbudeanu, L., Brici, I., Mare, C., Mihai, I. C., & Șcheau, M. C. (2021). Privacy Intrusiveness in Financial-Banking Fraud Detection. *Risks*, *9*(6), 104. https://doi.org/10.3390/risks9060104

Gilmour, P.M. (2022). Reexamining the anti-money-laundering framework: a legal critique and new approach to combating money laundering. *Journal of Financial Crime*, *30*(1), 35-47 https://www.emerald.com/insight/content/doi/10.1108/JFC-02-2022-0041/full/html

Greenlee, J., Fischer, M., Gordon, T., & Keating, E. (2007). An investigation of fraud in nonprofit Organizations: Occurrences and deterrents. *Nonprofit and Voluntary Sector Quarterly*, *36*(4), 676–694. https://doi.org/10.1177/089976400730040

Haddad, H. (2016). Internal controls in Jordanian banks and compliance risk. *Research Journal of Finance and Accounting*, *7*(24), 17–31. https://www.iiste.org/Journals/index.php/RJFA/article/download/34809/35825

Hamid, A., & Nasih, M. (2021). Fraud prevention of village funds in East Java Indonesia. *Management Science Letters*, 2033–2044. https://doi.org/10.5267/j.msl.2021.3.006

Handoyo, B. R. M., & Bayunitri, B. I. (2021). The influence of internal audit and internal control toward fraud prevention. *International Journal of Financial, Accounting, and Management*, *3*(1), 45–64. https://doi.org/10.35912/ijfam.v3i1.181

Hanoon, R. N., Khalid, A. A., Rapani, N. H. A., Aljajawy, T. M., & Al-Waeli, A. J. (2021). The impact of internal control components on the financial performance, in the Iraqi banking sector. *The journal of contemporary issues in business and government*, *27*(3), 2517-2529.

Hassan, M., Aziz, L. A. R., & Andriansyah, Y. (2023). The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics*, *6*(1), 110-132.

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 & Accounting*. https://doi.org/10.1108/jfra-05-2023-0235

IIA. (2019), "Position paper fraud and internal audit. Assurance over fraud controls fundamental to success", The Institute of Internal Auditors, p. 1.

Inaya, L., & Isito, E. O. (2016). An empirical analysis of social impact of fraud on the Nigerian banking industry. *Research Journal of Finance and Accounting*, *7*(4), 12-17.

International Finance Corporation [IFC]. (2021). Internal Control handbook. In *International Finance Corporation*. https://www.ifc.org/content/dam/ifc/doc/mgrt/ic-handbook-2021.pdf

Internal Control | COSO. (2023). COSO. https://www.coso.org/guidance-on-ic

Kamran, M., Miru, A., & Maskun, M. (2021). Online Selling And Buying Fraud: The Law Of Electronic Transaction Perspective. *JCH (Jurnal Cendekia Hukum)*, *6*(2), 270-288.

Kassem, R., & Higson, A. W. (2012). The new fraud triangle model. *Journal of Emerging Trends in Economics and Management Science*, *3*(3), 191–195. https://doi.org/10.10520/ejc132216

Kolapo, F. T., & Olaniyan, T. O. (2018). The Impact of Fraud on the Performance of Deposit Money Banks in Nigeria. *International Journal of Innovative Finance and Economics Research*, *1*(6), 40–49.

Koutoupis, A., & Malisiovas, T. (2021). The effects of the internal control system on the risk, profitability, and compliance of the U.S. banking sector: A quantitative approach. *International Journal of Finance & Economics*, *28*(2), 1638–1652. https://doi.org/10.1002/ijfe.2498

KPMG. (2013). *COSO Internal Control – Integrated Framework (2013)*. https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/2750-New-COSO-2013-Framework-WHITEPAPER-V4.pdf

Morgan, R. E. (2021). *Financial fraud in the United States, 2017*. US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics.

Murrar, F. (2021a). Fraud schemes during COVID-19: a comparison from FATF countries. *Journal of Financial Crime*, *29*(2), 533–540. https://doi.org/10.1108/jfc-09-2021-0203

Murrar, F. (2021b). Measures to combat money laundering and terrorist financing in Palestine. *Journal of Money Laundering Control*, *25*(2), 268–279. https://doi.org/10.1108/jmlc-02-2021-0010

Nuhaa, E., Aridahb, M. W., & Kamilb, G. A. (2021). The Effect of Applying COSO'S Internal Control Framework on Operational Risk Management in Commercial

Banks in Jordan. *Accounting and Management Information Systems AMIS 2021*, 244.

Nwaobia, A. N., Omotayo, I. I., & Ajibade, A. (2021). Internal audit and fraud detection in selected banks listed in Nigeria. *IOSR Journal of economics and Finance*, *12*(4), 51-65.

Nyakarimi, S. N., Kariuki, S. N., & Kariuki, P. W. ’. (2020). Risk assessment and fraud prevention in banking sector. *The Journal of Social Sciences Research*, *61*, 13–20. https://doi.org/10.32861/jssr.61.13.20

Occupational Fraud 2024: A Report to the Nations. (2024). In *www.acfe.com*. Association of Certified Fraud Examiners. https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf

Ogbeide, S. O. (2018). Empirical assessment of frauds on the financial performance of banking sector in Nigeria. *International Journal of Research Studies in Management*, *7*(1). https://doi.org/10.5861/ijrsm.2018.3007

Otoo, F. N. K., Kaur, M., & Rather, N. A. (2023). Evaluating the impact of internal control systems on organizational effectiveness. *LBS Journal of Management & Research*, *21*(1), 135–154. https://doi.org/10.1108/lbsjmr-11-2022-0078

Patterns of electronic fraud. (2024). In *Financial Follow-Up Unit*. FFU.

Paul, S. R., Haridas, M. K., & Prasad, K. D. V. (2023). BANK FRAUDS: AN EMPIRICAL ANALYSIS ON THE NEED FOR A ROBUST LEGAL MECHANISM. *Lex Humana (ISSN 2175-0947)*, *15*(2), 577-593.

Pcbs. (2023). *PCBS | Reported fraud offenses in Palestine by type of criminal Offense and Governorate, 2022*. https://www.pcbs.gov.ps/statisticsIndicatorsTables.aspx?lang=en&table_id=2031

Piskunov, V. A., & Tarasova, T. M. (2020). Internal Control and Internal Auditing Definitions. *Lecture Notes in Networks and Systems*, 726–735. https://doi.org/10.1007/978-3-030-60929-0_94

PMA Annual Report 2023. (2024). In *Palestine Monetary Authority (PMA)*. Research & Monetary Policy Department. https://www.pma.ps/Portals/0/Users/002/02/2/Publications/English/Annual%20Reports/PMA%20Annual%20Reports/Annual%20Report%202023.pdf?ver=2024-09-09-154309-437×tamp=1725885992947

Premti, A., Jafarinejad, M., & Balani, H. (2021). The impact of the Fourth Anti-Money Laundering Directive on the valuation of EU banks. *Research in International Business and Finance*, *57*, 101397. https://doi.org/10.1016/j.ribaf.2021.101397

prevent. (2025). In *Merriam-Webster Dictionary*. https://www.merriam-webster.com/dictionary/prevent

PricewaterhouseCoopers. (2021). *Fraud Risk Management*. PwC. https://www.pwc.co.uk/services/forensic-services/insights/fraud-detection-risk-management.html

PricewaterhouseCoopers. (2020). *PwC's Global Economic Crime and Fraud Survey 2020*. PwC. https://www.pwc.com/ua/en/survey/2020/economic-crime-survey.html

Rahman, R. A., & Anwar, I. S. K. (2014). Effectiveness of fraud prevention and detection techniques in Malaysian Islamic banks. *Procedia - Social and Behavioral Sciences*, *145*, 97–102. https://doi.org/10.1016/j.sbspro.2014.06.015

Rossi, D., & Lietz, T. (2022). Fraud Risk Assessment. In *The Institute of Internal Auditors*. IIA. https://www.theiia.org/globalassets/documents/chapters-and-

affiliates/north-america/united-states/georgia/atlanta/fraud-risk-assessment-presentation.pdf

Sabău, M. (2013). Fraud risk management-human rationalization assessment. *Business Excellence and Management*, *3*(1), 41-56.

Setyaningsih, P. R., & Nengzih, N. (2020). Internal control, organizational culture, and quality of information accounting to prevent fraud: case study from Indonesia's agriculture industry. *International Journal of Financial Research*, *11*(4), 316. https://doi.org/10.5430/ijfr.v11n4p316

Skula, I., Bohacik, J., & Zábovský, M. (2020, November). *Use of different channels for user awareness and education related to fraud and phishing in a banking institution*. 606–612. https://doi.org/10.1109/ICETA51985.2020.9379220

Sood, P., & Bhushan, P. (2020). A structured review and theme analysis of financial frauds in the banking industry. *Asian Journal of Business Ethics*, *9*(2), 305–321. https://doi.org/10.1007/s13520-020-00111-w

Sudirman, S., Sasmita, H., D, M. D., Krisnanto, B., & Muchsidin, F. F. (2021). Effectiveness of internal audit in supporting internal control and prevention of fraud. *Bongaya Journal of Research in Accounting*, *4*(1), 8–15. https://doi.org/10.37888/bjra.v4i1.271

The Institute of Internal Auditors [IIA]. (2019). Fraud and internal audit. In *The Institute of Internal Auditors*. The Institute of Internal Auditors (IIA). https://www.theiia.org/globalassets/documents/resources/fraud-and-internal-audit-assurance-over-fraud-controls-fundamental-to-success-april-2019/fraud-and-internal-

audit.pdf#:~:text=Operationally,%20internal%20audit%20should%20have%20sufficient%20knowledge%20of%20fraud%20to:

Team, C. (2023, October 3). *Internal controls*. Corporate Finance Institute. https://corporatefinanceinstitute.com/resources/accounting/internal-controls/

Tomaš, D., & Todorović, I. (2016). Modelling Fraud Prevention Process **. *Journal of Corporate Governance Insurance and Risk Management*, *3*(2), 76–87. https://doi.org/10.56578/jcgirm030205

Vassiljev, M., & Alver, L. (2016, December). Conception and periodisation of fraud models: Theoretical review. In *5th International Conference on Accounting, Auditing, and Taxation (ICAAT 2016)*. Atlantis Press.

Vicente, V. (2023, April 21). *What is a fraud risk assessment? and why do I need one?* Auditboard. https://www.auditboard.com/blog/what-is-fraud-risk-assessment/

Vijeyan, S., & Rahmat, M. M. (2022). Effects of Internal Control towards Money Laundering Prevention: An Interrelation Perspective. *Asian Journal of Accounting and Governance*, *17*, 13-25.

Wanjala, K., & Riitho, D. G. (2020). Internal Control Systems Implementation and Fraud Mitigation Nexus among Deposit Taking Saccos in Kenya. *Finance & Economics Review*, *2*(1), 11–29. https://doi.org/10.38157/finance-economics-review.v2i1.59

Warning of electronic fraud. (2018). Financial Follow-Up Unit. https://www.ffu.ps/ar/Article/46/%D8%AA%D8%AD%D8%B0%D9%8A%D8%B1-%D9%85%D9%86-%D8%B9%D9%85%D9%84%D9%8A%D8%A7%D8%AA-%D8%A7%D9%84%D8%A7%D8%AD%D8%AA%D9%8A%D8%A7%D9%8

4-
%D8%A7%D9%84%D8%A7%D9%84%D9%83%D8%AA%D8%B1%D9%88
%D9%86%D9%8A

Wells, J. T. (2014). Principles of Fraud Examination (4th ed.). *Wiley*. Chapter 1. P.8.

Zamzami, F., Nusa, N. D., & Timur, R. P. (2016). The effectiveness of fraud prevention and detection methods at universities in Indonesia. *DOAJ (DOAJ: Directory of Open Access Journals)*.
https://doaj.org/article/cd2090353cc3486b84e844135034d953

Appendices

Appendix (1): Questionnaire of the Study

الجامعة العربية الأمريكية
ARAB AMERICAN UNIVERSITY

Greetings,

As part of my master's degree studies in *Fraud Protection* at the Arab American University, I have prepared this questionnaire as part of the academic research requirements. The purpose of this questionnaire is to collect data and information that will help analyze the role of internal controls in preventing and detecting fraud in Palestinian banks, which is the focus of my study.

Your participation in this questionnaire is very important to the success of the research, as it will provide valuable insights that contribute to achieving accurate and reliable results. Please be assured that all answers provided will remain completely confidential, and the data will be used solely for scientific research purposes.

Please note that answering the questions is optional, and you may withdraw at any time if you wish to do so. We highly appreciate your time and effort in helping make this research successful.

Thank you for your cooperation and continued support.

Best regards,
Aseel Alzaqlih
Master's Student in Fraud Protection

Mobile: 0597377273
Email: aseel.alzaqlih@gmail.com
Arab American University

Section One: Demographic Information

Gender:

☐ Male ☐ Female

Age Group:

☐ 20–30 years ☐ 31–40 years ☐ 41–50 years ☐ Over 50 years

Educational Level:

☐ Diploma ☐ Bachelor’s ☐ Postgraduate ☐ Other (specify)

Years of Experience in Control Departments:

☐ Less than 1 year ☐ 1–5 years ☐ 6–10 years ☐ More than 10 years

Job Level:

☐ Employee ☐ Supervisor/Head of Department ☐ Deputy Manager ☐ Manager

Bank Name:

Section Two: Please mark the appropriate answer

Increase in Fraud Cases Targeting Bank Customers and the Reasons Behind It			
Paragraph	**figure**	**Yes**	**No**
1	Have you ever heard of bank fraud cases		
2	Do you think that bank fraud has increased recently		
3	Fraud cases reported to banks by customers represent a very small percentage of actual fraud cases.		

figure	Paragraph	Strongly agree	I agree	neutral	Disagree	Strongly disagree
4	Technological advancements, the expansion of the internet, and businesses' reliance on this technology have caused the number of fraud cases to rise.					
5	The ongoing war in Gaza and the population's need for aid have caused the number of fraud cases to rise.					
6	Lack of security awareness among bank customers has caused the number of fraud cases to rise.					
7	The rise in organized crime and the greed for money has caused the number of fraud cases to rise.					

Fraud Protection Controls						
figure	**Paragraph**	**Strongly agree**	**I agree**	**neutral**	**Disagree**	**Strongly disagree**
8	The bank has controls in place to prevent and mitigate fraud.					
9	Control mechanisms are implemented to detect fraud cases when they occur.					
10	Corrective measures are taken to ensure that detected fraud cases do not recur and to correct deviations.					
11	The bank's senior management periodically reviews and evaluates the effectiveness of internal controls.					
12	Banks conduct customer awareness campaigns regarding fraud.					
13	Fraud risks are assessed periodically and continuously to identify, analyze, and manage these risks appropriately.					
The Relationship Between Regulatory Controls and Fraud Prevention						
figure	**Paragraph**	**Strongly agree**	**I agree**	**neutral**	**Disagree**	**Strongly disagree**
14	Effective internal controls play a role in fraud prevention within the bank.					

15	Educating customers about fraud topics and common methods leads to reduce exposure to fraud.					
16	Using two-factor authentication to access data helps reduce the incidence of fraud.					
17	Banks protecting their systems and devices used to implement banking services reduces exposure to fraud.					
18	In your opinion, which of the following areas can internal control most effectively help reduce fraud					
A.	Controlling access to data and financial systems.					
B.	Periodically reviewing financial transactions.					
C.	Investigating complaints and reports related to fraud.					
D.	Ensuring that policies and procedures are properly implemented.					
E.	Other (Select)					

The Relationship Between Controls and Fraud Detection						
figure	**Paragraph**	**Strongly agree**	**I agree**	**neutral**	**Disagree**	**Strongly disagree**
19	Effective internal controls enable the bank to detect fraud early.					
20	The bank's use of advanced technical systems (automated transaction monitoring systems) leads to fraud detection.					
21	Training employees on controls related to fraud detection helps detect it more effectively.					
22	In your opinion, which of the following actions should institutions take to improve the effectiveness of internal controls in detecting fraud					
A.	Increasing coordination between different departments.					
B.	Improving internal investigation procedures.					
C.	Regularly reviewing and updating controls.					
E.	Other (Select)					
Observations						
If you have any other comments, please include them below:						

ملخص الدراسة

هدفت هذه الدراسة إلى التحقيق في العلاقة بين الرقابة الداخلية والاحتيال داخل البنوك المحلية الفلسطينية. ويتمثل هدفها الأساسي في استكشاف واقع حالات الاحتيال، وأسبابها، والرابط بين أنظمة الرقابة الداخلية القوية وفعاليتها في منع هذه الجرائم واكتشافها على حد سواء، تُعد هذه الدراسة واحدة من الدراسات القليلة التي تحقق على وجه التحديد في واقع الاحتيال في فلسطين.

تنتمي هذه الدراسة الى حقل الدراسات السببية، واعتمدت على المنهج المختلط (كمي ونوعي)، تم جمع البيانات من عينة مكونة من 67 موظفًا تم اختيارهم بطريقة قصدية (عينة غير احتمالية) لضمان مجموعة سكانية متنوعة ديموغرافيًا بناءً على متغيرات مثل الجنس والفئة العمرية والمستوى التعليمي، تم توزيع 67 استبيانًا بالمجمل، وجميعها كانت صالحة وتم استردادها، مما اظهر نسبة استجابة بلغت 100%، تهدف النتائج إلى تقديم رؤى قيمة للبنوك الفلسطينية لتعزيز بيئات الرقابة لديها وزيادة مرونتها في مواجهة الأنشطة الاحتيالية.

اظهرت نتائج هذه الدراسة تزايد حالات الاحتيال داخل البنوك المحلية الفلسطينية، بسبب نقص الوعي الأمني لدى العملاء، والطمع في تحقيق أرباح سريعة، والاعتماد المتزايد على خدمات البنوك الإلكترونية، كما اظهر البحث ايضاً وجود فجوة بين حالات الاحتيال المبلغ عنها والحالات الفعلية.

كما تُسلط الدراسة الضوء على تأثير التطورات التكنولوجية والتحديات السياسية والاقتصادية، مثل حرب غزة، وتكشف أن البنوك الفلسطينية تستخدم بشكل فعال نظام رقابة داخلية شاملة، يشمل تقييمات مخاطر الاحتيال، وحملات التوعية للعملاء، وتدريب الموظفين، لمنع الاحتيال واكتشافه.

بالإضافة إلى ذلك، تؤكد النتائج على وجود علاقة قوية وعكسية بين ضوابط الرقابة الداخلية القوية والاستعداد للاحتيال، مما يبرز أن استراتيجية الدفاع متعددة الأوجه ضرورية، تشمل هذه الاستراتيجية إجراءات تكنولوجية مثل المصادقة الثنائية، والمراقبة المستمرة للضوابط، وأنظمة الكشف المتقدمة، والتي تشكل معًا إطارًا مرنًا لحماية العمليات المصرفية والتخفيف من التهديد المتطور للاحتيال المالي.

واستنادًا إلى استنتاجات الدراسة، اقترح الباحث أن البنوك تحتاج إلى تعزيز منع الاحتيال من خلال تطوير سياسات شاملة لمكافحة الاحتيال، وإنشاء فريق متخصص لمتابعة حالات الاحتيال وكشفها، وتنفيذ أنظمة كشف متقدمة تعمل بالذكاء الاصطناعي.

علاوة على ذلك، فإن تعزيز وعي كل من العملاء والموظفين من خلال التدريب المستمر، وتحسين إجراءات الأمان التكنولوجي مثل المصادقة البيومترية، وايجاد ضوابط تشغيلية أكثر صرامة مثل تحديد سقوف العمليات المالية، هي إجراءات أساسية، تهدف هذه الإجراءات المتكاملة إلى إنشاء نظام دفاع قوي ومتعدد الطبقات للتخفيف بشكل كبير من مخاطر الاحتيال.