



Review

Structured Framework for Dealing with Types of Financial Statement Fraud, Integrating Common Modalities, Variables, Strategies, and Patterns

Ludivia Hernandez Aros ^{1,2,*}, José Jimmy Sarmiento Morales ¹ and John Johver Moreno Hernández ²

¹ Business School, Universidad de La Salle, Bogotá 110211, Colombia; josarmiento@lasalle.edu.co

² Faculty of Economic, Administrative and Accounting Sciences, Universidad Cooperativa de Colombia, Ibagué-Tolima 730001, Colombia; john.morenoh@campusucc.edu.co

* Correspondence: lhernandez70@unisalle.edu.co or ludivia.hernandez@campusucc.edu.co

Abstract

This article proposes a structured framework for financial statement fraud in five dimensions, nature of fraud, execution, participation, organizational impact, and environment, which are broken down into variables and subvariables to describe and analyze this phenomenon systematically. Based on a conceptual review and systematization, a structure is proposed that encompasses the diversity of intentions, motivations, methods, and actors involved, considering human and automated factors in current organizational contexts marked by digitization and increasing regulatory complexity. The framework also highlights the relevance of variables such as the persistence of fraud, technical capacity of fraudsters, and the level of internal/external collusion, integrating elements of internal control, corporate culture, and early warning signs. This framework provides a methodological basis that facilitates the design of more robust prevention, detection, and monitoring strategies, contributing to auditing practices, corporate governance, and strengthening control systems. Limitations to the need for empirical validation are identified, and future lines of research are suggested, aimed at applying data analysis, and artificial intelligence to address increasingly sophisticated fraud schemes.

Keywords: financial statement fraud; auditing; nature of fraud; fraud variables; collusion; prevention strategies; detection strategies; monitoring strategies

1. Introduction

Financial statement fraud is one of the most damaging forms of fraud, characterized by the exploitation of an organization's resources by internal and external individuals for their own benefit (Ashtiani & Raahemi, 2022). According to the Association of Certified Fraud Examiners (ACFE), the annual financial impact of fraud exceeds \$5 trillion worldwide, reflecting detailed figures in its 2024 Global Fraud Survey, with a total of 1921 cases analyzed, occurring between January 2022 and September 2023, compiled from professionals in 138 countries. Overall, 89% of frauds corresponded to misappropriation of assets (average loss of \$120,000); corruption represented 48% (average loss of \$200,000); and notably, fraud in financial statements accounted for 5% of cases and an average loss of \$766,000. Notably, the sum of the percentages does not reach 100% because the categories of fraud are not mutually exclusive; that is, the same case may involve embezzlement, corruption, or financial statement fraud simultaneously, resulting in overlap between them. Between 2022 and 2024, average losses increased by 29% for financial statement fraud, 33%



Academic Editors: Thanasis Stengos and Justin Y. Jin

Received: 6 December 2025

Revised: 3 January 2026

Accepted: 9 January 2026

Published: 19 February 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

for corruption, and 20% for asset misappropriation, reflecting an alarming trend in the occurrence of fraud (ACFE, 2024).

From a broader theoretical perspective, financial sustainability and the risk of organizational failure constitute critical contextual factors in the emergence of fraudulent financial reporting. Firms facing financial distress, declining performance, or heightened bankruptcy risk often operate under intensified economic and reputational pressure, which may distort managerial judgment and increase incentives to manipulate accounting information. Prior research suggests that such conditions can weaken internal controls, exacerbate agency conflicts, and foster opportunistic behavior aimed at preserving short-term viability or delaying negative market reactions (Srebro et al., 2021). Consequently, understanding fraud in financial statements requires not only the identification of manipulation techniques, but also an examination of the structural and financial conditions under which fraudulent behavior becomes more likely.

Based on the above, understanding the nature and diverse types of fraud in financial statements is essential for designing effective prevention, detection, and mitigation strategies. Over the last few decades, research in this area has made considerable progress on the determinants of fraud, associated organizational behavior profiles, and techniques used to distort financial information (Onwubiko, 2020). However, despite these advances, fraud in financial statements is a latent threat in markets around the world. Its dynamic nature and the increasing sophistication of fraudulent methods challenge traditional control and audit systems, highlighting the need to develop conceptual/analytical frameworks and technological tools for its timely detection.

In view of the above, the objective of this article is to strengthen the existing theoretical framework by formulating a conceptual framework that integrates and categorizes the main types of fraud in financial statements and the behavioral and organizational patterns that underpin it. Thus, the purpose of the structured classification is to lay solid conceptual foundations that will guide future empirical research and facilitate a comprehensive understanding of the phenomenon under study. It also proposes prevention and monitoring strategies that enable auditors, regulators, and corporate governance officials to strengthen internal control systems, mitigate emerging risks, and respond proactively to new dynamics and modalities of fraud in financial statements.

2. Background

The study of financial statement fraud can be traced back to the South Sea Bubble case in England in 1720, where executives manipulated accounting records to appropriate shares, ruining thousands of investors (Wan, 2024). That episode set a precedent by highlighting the lack of regulation and supervision, as it provided opportunities for large-scale fraudulent schemes. In the 19th century, crises, such as the English banking crisis of 1825 and the Horatio Bottomley fraud, reinforced control mechanisms (Cox & Mowatt, 2019), resulting in lax penalties, with no one responsible for the Bubble facing prison (Wan, 2024).

Among investigations into financial statement fraud, the cases of Enron, Lehman Brothers, Madoff, WorldCom, and Barings Bank highlight the importance of ethics, transparency, and adequate regulation in organizations. Enron concealed debts and inflated revenues, leading to its collapse in 2001 (Munawer et al., 2012), while Lehman Brothers employed deceptive accounting practices that contributed to the 2008 monetary crisis (Mensah, 2012; Mohammed, 2023). Madoff defrauded thousands of investors through a Ponzi scheme worth more than \$65 billion (Clauss et al., 2009; Dimmock & Gerken, 2011), while WorldCom manipulated expenses to inflate revenues and filed for bankruptcy in 2002 after it was revealed that it had inflated its assets by nearly \$11 billion (Petra & Spieler, 2020; Scharff, 2005). Similarly, Barings Bank collapsed due to unauthorized trad-

ing (Petra & Spieler, 2020; Scharff, 2005). These cases highlight the weakness of effective internal controls, the lack of external auditors, and advanced AI tools to prevent fraud and ensure financial transparency, although in many of the cases mentioned, corporate governance approval was in place.

As a result of the fraud, a regulatory response was generated that included the Sarbanes-Oxley Act (SOX) in 2002, which required greater transparency in financial reporting and criminal liability for executives (Lee, 2024; Nazarova et al., 2020). As a result, provisions of IAS 240 reinforced the role of auditors in detecting irregularities (Bandara & Faltá, 2021; Johri, 2024). In turn, the creation of the Public Company Accounting Oversight Board (PCAOB) (USA) and the adoption of IFRS sought to standardize accounting practices to reduce fraud in financial statements (Christensen et al., 2024; Robles Quiñónez et al., 2024).

3. Related Works

Throughout the literature, fraud has been extensively examined in terms of its typologies, drivers, and detection mechanisms due to its significant impact on organizational financial performance. While prior studies have made important contributions, the existing research reveals several unresolved conceptual and integrative gaps that motivate the present study. To provide a coherent overview of these contributions, the following discussion is organized according to the dominant analytical orientation of prior studies. Specifically, the literature is examined by distinguishing between works that emphasize fraud detection techniques, those that focus on the structural or typological characterization of fraud, and studies that synthesize methodological trends through systematic or bibliometric reviews. This organization facilitates a clearer understanding of how existing research approaches financial statement fraud from different, yet complementary, perspectives.

West and Bhattacharya (2016) analyze financial fraud detection across multiple sectors and emphasize the growing relevance of computational intelligence techniques. However, their focus is primarily methodological, addressing detection algorithms rather than the conceptual organization and classification of fraudulent schemes within accounting and financial reporting contexts. Similarly, Reurink (2018) proposes a broad classification of financial fraud based on markets, financial instruments, and actors involved, offering valuable insights into structural conditions that facilitate fraud, yet without providing a systematic framework tailored to financial statement fraud or accounting records.

Onwubiko (2020) develops a comprehensive taxonomy of fraud using morphological analysis, covering characteristics, actors, intentions, and methods. Although analytically robust, this taxonomy is not specifically designed to classify fraudulent schemes as they manifest in financial statements, limiting its direct applicability to accounting-focused analysis. More recent studies by Hilal et al. (2022), Shahana et al. (2023) and Hernandez et al. (2024) concentrate on fraud detection using artificial intelligence and machine learning techniques, providing systematic and bibliometric reviews of models, datasets, and performance metrics. These studies typically treat fraud categories as predefined inputs and devote limited attention to the conceptual foundations and consistency of fraud classifications.

Despite differences in scope, methodology, and analytical emphasis, the reviewed studies converge in revealing a common limitation: the lack of an integrative perspective that explicitly connects fraud typologies with accounting-specific manifestations and analytical dimensions relevant for classification and detection. Detection-oriented research often relies on predefined fraud categories, whereas typological studies frequently remain detached from practical accounting applications. This gap underscores the need for a structured conceptual synthesis capable of bridging these strands of literature.

Overall, the reviewed literature highlights fragmentation between high-level fraud typologies, accounting-specific characteristics, and detection-oriented research. Existing

studies tend to emphasize either technological detection methods or broad classifications, without integrating recurring conceptual dimensions into a structured framework specifically focused on fraudulent schemes in accounting and financial statements. Addressing these gaps, the present study synthesizes convergent classification elements reported across the literature to propose a structured conceptual framework aimed at characterizing and supporting the detection of fraudulent schemes in accounting and financial reporting contexts.

Literature Identification and Analytical Approach

The conceptual framework proposed in this study is grounded in a structured and theory-driven review of the academic literature on financial statement fraud. The literature was identified through targeted searches of peer-reviewed journal articles addressing accounting manipulation, financial reporting fraud, fraud typologies, and detection frameworks. Attention was given to studies that explicitly propose classifications, analytical dimensions, or explanatory constructions related to fraudulent behavior in financial reporting contexts.

The selection of studies followed relevance-based criteria rather than an exhaustive systematic protocol. Specifically, articles were retained when they (i) focused on fraud affecting financial statements or accounting disclosures, (ii) contributed conceptual models, taxonomies, or analytical dimensions applicable to fraud characterization or detection, and (iii) were recurrently cited or theoretically influential within the fraud and accounting literature. This approach ensured conceptual saturation by emphasizing convergent findings and recurring constructs across independent studies.

Rather than aggregating empirical results, the reviewed literature was analyzed comparatively to identify common classification logics, shared explanatory dimensions, and persistent gaps in existing fraud models. These recurring elements were synthesized to construct an integrative framework that reconciles fragmented typologies and provides a structured representation of financial statement fraud. This analytical process enhances the internal coherence, transparency, and conceptual reliability of the proposed framework, while remaining consistent with the exploratory and integrative nature of a conceptual review.

4. Structured Framework

This section proposes a structured framework for the typology of fraud in financial statements, classifying them according to our own analysis developed from the scientific RSL on fraud in financial statements, with the integration and synthesis of various theoretical and empirical approaches, where conceptual patterns were identified that allowed the manifestations of fraud to be grouped into five categories as follows:

1. Fraud through accounting manipulation;
2. Fraud through omission or misleading disclosure;
3. Fraud through concealment technology;
4. Sectoral and structural fraud;
5. Fraud through justification/rationalization.

From an analytical standpoint, the proposed categories are organized as a stable and mutually exclusive classification, designed to support both empirical analysis and professional application. Each category represents a dominant mode through which financial statement fraud manifests, while the associated dimensions and variables operate as analytical attributes that allow individual cases to be consistently classified within the same typological structure. This design ensures that the framework can be applied across different organizational contexts without altering its internal logic.

In practical terms, the framework enables analysts, auditors, and researchers to operationalize the taxonomy by sequentially mapping observed accounting irregularities to the relevant category and then refining the analysis through the associated variables (e.g., intention, motivation, persistence, and implementing agency). This stepwise classification logic facilitates empirical coding, comparative case analysis, and integration into forensic audits or data-driven fraud detection systems. By explicitly linking categories, variables, and analytical use cases, the framework articulates a coherent taxonomy rather than a descriptive list of fraud manifestations.

Therefore, the conceptual framework and the proposed classification of fraudulent schemes are grounded in recurring typologies, mechanisms, and explanatory dimensions consistently reported in the literature. The studies cited in this section were identified through a structured review of peer-reviewed journal articles focusing on financial statement fraud, accounting manipulation, and fraud classification or detection models. Specifically, these studies were selected because they explicitly describe fraud typologies, classification criteria, or underlying mechanisms relevant to accounting and financial reporting contexts.

The information extracted from these studies included definitions of fraud categories, descriptions of fraudulent schemes, and the analytical dimensions used to differentiate types of fraud (e.g., intent, actors involved, manipulation techniques, and reporting outcomes). The proposed framework was constructed by synthesizing convergent classification elements repeatedly observed across these sources, rather than relying on a single model or author, thereby ensuring conceptual robustness and alignment with established fraud literature (Bhattacharya & Mickovic, 2024; Boddy et al., 2024; Bustamante et al., 2025; Hernandez et al., 2024; Hilal et al., 2022; Hudayati et al., 2022; Musfi & Soemantri, 2024; Onwubiko, 2020; Ranganatha & Syed Mustafa, 2025; Reurink, 2018; Shahana et al., 2023; West & Bhattacharya, 2016).

The proposed framework covers the general types of financial statement fraud (Figure 1). Unlike existing fraud models, which often focus on isolated fraud typologies or detection techniques, the proposed framework provides an integrated classification specifically tailored to accounting manipulation and intentional distortions in financial reporting. This section explains the categories used based on the type of accounting manipulation or intentional distortion of financial information, synthesizing recurring classification elements identified across prior studies into a coherent structure. Therefore, the first stage of the methodology consists of categorizing each case according to the nature of the financial statement fraud.

4.1. Classification and Mapping of Fraud in Financial Statements

Analyzing the origin of fraud in financial statements is challenging due to the complexity and volume of accounting records, financial reports, and administrative data. To address this, fraud has been categorized by type and subtype, allowing forensic auditors and accounting professionals to more accurately identify the mechanisms used by fraudsters to alter financial information. This approach promotes the analysis and monitoring of each case, becoming a tool for detecting/preventing illegal behavior.

Based on the literature, different patterns have been identified that classify forms of fraud in financial statements. These types are not mutually exclusive: a particular case may contain elements from several categories. For example, income is combined with the omission of liabilities or manipulation of explanatory notes. This structured classification serves as the basis for accounting review techniques (Demetriades & Owusu-Agyei, 2022; W. Lu & Zhao, 2021). Figure 2 presents a detailed categorization of the types of fraud in financial statements proposed in this article, which is particularly relevant in contexts where

transparency and accountability are essential. This organization strengthens institutional oversight, develops more robust corrective and preventive measures, and preserves the integrity of financial information.

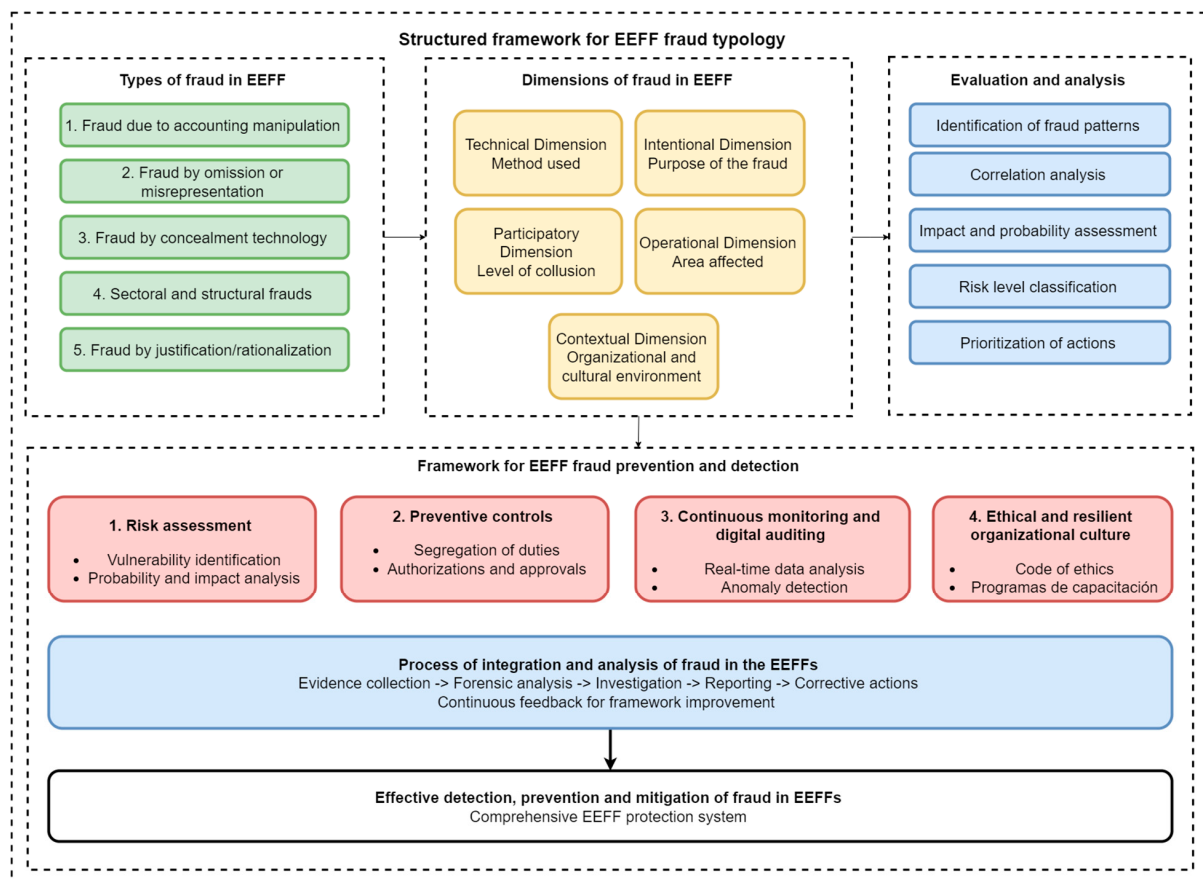


Figure 1. Structured framework of the types of fraud in financial statements. Source: Authors.

The categorization of fraud in financial statements is a step toward developing effective detection, control, and prevention mechanisms in the accounting and financial fields. As fraudulent practices become more sophisticated, it is essential to analyze the ways in which they manifest themselves, considering the methods used and the structural and institutional context that enables them. At the same time, the literature has proposed various classifications that group frauds according to their nature, technique used, and motivations. Five categories have been identified, each with distinct characteristics, but not mutually exclusive.

Firstly, accounting fraud is one of the most traditional and widespread forms of financial statement manipulation. This type of fraud involves the intentional modification of financial records with the aim of altering the perception of the entity's economic situation, thereby influencing the decision-making of stakeholders. Additionally, the most common strategies include recognizing fictitious income, omitting liabilities, and overvaluing assets, thereby creating a distorted image of the organization's actual financial position (Bhattacharya & Mickovic, 2024; Rahman & Zhu, 2024).

A second category corresponds to fraud by omission or misleading disclosure, which operates on the narrative and explanatory elements of financial statements, such as notes or audit reports. Although fraud lies in altered figures, deliberate omission of facts, and distortion of contextual information, it reduces information transparency and restricts the ability of external users to analyze and interpret the information (Musfi & Soemantri, 2024; Vizcarra, 2019).

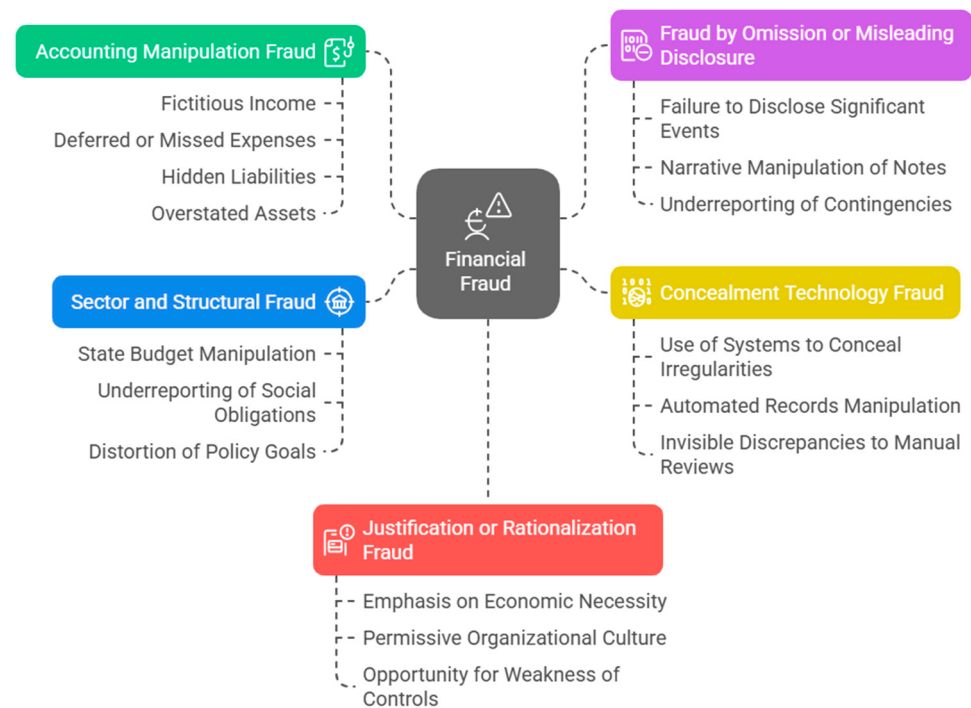


Figure 2. Classification of fraud in financial statements. Source: Authors' own elaboration based on the literature review.

Likewise, advances in digital technologies have generated a third emerging category: concealment technology fraud. This involves computer tools used to manipulate, delete, or conceal automated or systematic accounting information, consisting of altering accounting databases, designing algorithms that modify reports in real time, or software to erase electronic traces of unrecorded transactions. This scenario favors automation-related technologies, including big data and AI, which are no longer neutral tools but have become facilitators of fraudulent behavior (Cugniere et al., 2022; Ranganatha & Syed Mustafa, 2025).

On the other hand, sectoral or structural fraud refers to illegal practices linked to the functioning and institutional logic of the public/private sectors. In the public sector, it manifests itself in the intentional underreporting of tax obligations, the manipulation of official budgets, or the distortion in the allocation and execution of transfers and subsidies. In the private sector, it takes the form of systematic evasion or concealment of related-party transactions; fraudulent conduct embedded in complex institutional structures that consolidate its persistence and make it difficult to detect (Baumgärtler et al., 2024; Boddy et al., 2024).

However, a less visible category of fraud has been identified: justification/rationalization. This is based on individual motivations and subjective perceptions that legitimize or minimize the seriousness of the fraudulent act. Among the most common are pressures to meet performance targets, the need to keep one's job, and the existence of an organizational culture that is permissive and even promotes ethically questionable practices. Thus, internal justifications function as triggers for fraudulent behavior and contribute to its normalization within certain corporate environments (Hudayati et al., 2022; Parlindungan et al., 2017).

In accordance with the above, this categorization systematically composes the phenomenon of fraud in financial statements, recognizing its typological diversity and the technological, organizational, and institutional factors that influence its occurrence. It also serves as input for designing audit strategies that are more focused and adaptable to new emerging risks in increasingly digitized and complex contexts.

A conceptual clarification is required regarding the role of intention within the proposed framework. In line with classical fraud theory, intentionality constitutes a defining

element of fraud, as fraudulent acts necessarily involve deliberate misrepresentation or concealment. Accordingly, the category labeled as “accidental” does not imply the existence of fraud without intent. Rather, it is incorporated analytically to distinguish non-deliberate accounting distortions—such as errors, misjudgments, or misapplications of standards—that may initially resemble fraudulent outcomes but lack malicious intent. This distinction is critical for forensic and auditing purposes, as it allows practitioners to differentiate intentional fraud from negligence or error during investigative stages.

Furthermore, the framework deliberately separates descriptive classification variables from explanatory or interpretative dimensions. While certain components of the model describe observable characteristics of fraudulent schemes (e.g., nature of manipulation, persistence, implementing agency), other dimensions—such as motivation, purpose, or rationalization—serve an analytical function aimed at explaining why fraudulent behavior occurs. These explanatory dimensions are not treated as fraud types per se, but as contextual drivers that interact with fraud mechanisms. This layered structure avoids conceptual conflation by preserving a clear analytical distinction between the form of fraud and the underlying behavioral or organizational factors that enable it.

On the other hand, the typology of fraud in financial statements is a complex construction determined by interrelated variables that classify and detect the mechanisms through which fraudulent practices are perpetuated; these variables are classified into five dimensions: intent, method, collusion, affected area, and context (Table 1).

To understand the dynamics of fraud in financial statements, five categories are proposed, each linked to a specific dimension that defines and examines its characteristics and constitutes a conceptual structure that facilitates the identification, classification, and analysis of fraudulent manifestations in organizational contexts, providing a basis for their detection and prevention through advanced tools such as digital auditing and AI. Table 2 summarizes this relationship:

Based on this classification, each category is examined in depth to explain its characteristics and how they manifest themselves in financial statement fraud schemes. Therefore, analyzing nature, execution, participation, organizational impact, and environment establish a framework that supports the design of detection and control strategies. Each category is detailed below, along with its associated dimension.

Table 1. Dimensions and their variables.

Category	Dimension	Variable	Sub Variable	Description	Characteristics	Strategies
1. Nature of fraud	Intention	Type of intent	—	Level of premeditation of fraud.	Malicious, not malicious, and accidental.	Analysis of behavioral patterns, evaluation of accounting judgments.
		Motivation	—	Reason or incentive driving fraud.	Financial (profits), non-financial (reputation).	Interviews, analysis of pressures and incentives.
		Purpose of the fraud	Improving the financial image	Manipulation to attract investors or meet internal goals.	Inflating revenues, hiding liabilities.	Forensic analysis of financial goals, review of economic rationality
			Reduce the tax burden	Tax evasion through accounting manipulation.	Underreporting income, fictitious expenses.	
		Persistence	—	Whether fraud is ongoing or a one-time occurrence.	Transitory (single), permanent (recurring).	Continuous monitoring, recurring audit

Table 1. Cont.

Category	Dimension	Variable	Sub Variable	Description	Characteristics	Strategies
1. Nature of fraud	Intention	Capacity of the fraudster	—	Technical and organizational level of the fraud perpetrator.	Level of ability: low, medium, or high, depending on the fraudster's expertise. Ability to defraud limited, competent, or significant.	Assessment of access profiles and technical skills
		Implementing agency	—	Individual or collective actor who committed the fraudulent act.	Human, bot, Robotic Process Automation (RPA), script, malware.	Evaluation of access profiles, traceability of digital activity
2. Execution of fraud	Method	Technique used	Accounting manipulation	Intentional alteration of financial figures.	Change in accounting policies, improper recognition.	Development of intelligent solutions based on AI and RPA to optimize the review of accounting records, detect anomalous patterns, and expose fraud schemes.
			Document forgery	Manufacture or falsification of documents.	Fake invoices, altered contracts.	
			Omission of information	Failure to declare or register key items.	Hidden liabilities, overlooked risks.	
		Channel	—	Means by which fraud is committed.	Web, mobile, telephony, physical.	Multi-channel supervision, monitoring of electronic transactions
		Rules violated	—	Rules or laws are broken.	IFRS, GAAP, SOX, tax regulations. Internal regulations Internal control	Regulatory compliance verification, legal compliance, and internal control audit
		Impact on financial statements	—	How fraud distorts financial statements.	Accounting manipulation, concealment of losses or risks.	Analysis of significant variations, substantive tests, and control tests
3. Participation	Level of Collusion	Level of participation	Individual	A single person commits the fraud.	Employees with uncontrolled access.	Mapping of key actors, collusion analysis, and analysis of factors such as access to accounting records, employee capability, and opportunity to perpetrate fraud
			Interna	Several employees in collusion.	E.g., Accountant + treasurer + CEO + others.	
			Externa	Participation of third parties outside the company.	Example: Supplier, corrupt auditor	
		System limit	—	Where the fraud originates.	Internal (within the organization), external.	Analysis of access origin, segregation of duties
		Roles involved	—	People or roles involved.	Managers, auditors, operators.	Assessment of critical functions, rotation of sensitive personnel Analysis of the profile of those involved

Table 1. Cont.

Category	Dimension	Variable	Sub Variable	Description	Characteristics	Strategies
4. Organizational impact	Affected area	Type of impact	Revenue	Fraud that alters sales or collections.	Fictitious sales, double invoicing.	Accounting materiality analysis, financial scenario simulation, analysis of historical financial indicators
			Expenses/Purchases	Manipulation of costs or payments.	Fictitious suppliers, bribes.	
			Assets	Inflation or appropriation of assets.	Inflated inventory, covert theft.	
			Liabilities	Concealment or underestimation of debts.	Omit loans, litigation.	
		Amount involved	—	Economic value related to fraud.	High, moderate, low.	Evaluation of significant transactions, integrity tests, and substantive tests
		Implementation period	—	Temporary duration of the fraud.	Short, prolonged, chronic.	Time series comparison, seasonality adjustment
5. Environment and signs	Context	Culture and internal control	—	Environments that facilitate fraud.	Perverse incentives, weak controls.	Organizational climate diagnosis, internal control assessment
		Warning indicators	—	Visible or detectable signs of fraud.	Frequent auditor changes, recurring inconsistencies.	Early warning systems, use control panels to minimize risks. Use of models that integrate AI for early prevention
		Operational context	—	Pressures, weaknesses, or organizational environment.	Crisis, pressure to meet targets, lax supervision.	Analysis of the control of environment, evaluation of strategic processes

Source: Authors. Note: Own adaptation based on the RSL (Dellaportas, 2013; Gray & Debreceeny, 2014; Leistedt & Linkowski, 2016; Marquart & Thompson, 2024; Onwubiko, 2020).

Table 2. Category and scale associated with fraud in financial statements.

Category	Associated Dimension
Nature of fraud	Intent
Execution of fraud	Method
Participation	Level of Collusion
Organizational impact	Area Affected
Environment and signs	Context

Source: Authors.

4.1.1. First Category: Nature of Fraud—Dimension: Intent

The nature of fraud is defined by the intent underlying the criminal act, which examines the premeditation and deliberate willingness to manipulate accounting information to obtain undue benefits, evade responsibility, or misrepresent the entity's financial situation (Onwubiko, 2020). Thus, identifying intent makes it possible to differentiate between unintentional accounting errors and fraudulent acts and supports the design of ethical and regulatory control mechanisms within organizations.

As shown in Figure 3, the intentional dimension categorized by the nature of fraud identifies factors such as the fraudster's intent, motivation, persistence, opportunity, level of technical and organizational capability, and the executing entity (human or automated); These factors help auditors and accounting professionals anticipate risks, strengthen internal controls, and develop more effective prevention and detection strategies.

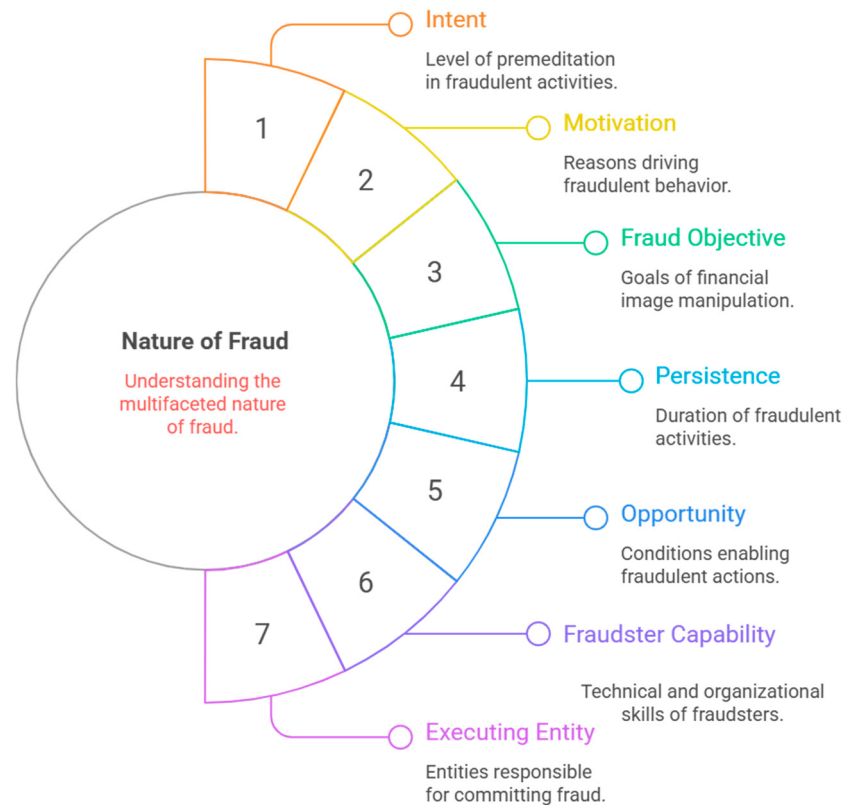


Figure 3. Variable: intentional dimension of fraud. Source: Authors.

To begin with, the intent behind a fraudulent act is one of the key factors in its classification, analysis, and subsequent treatment from an accounting and auditing perspective (Onwubiko, 2020). The type of intent refers to the level of premeditation with which fraud is conceived and executed and directly influences its detection, risk assessment, and determination of legal and ethical responsibilities. Thus, three categories are identified: (1) malicious fraud, (2) non-malicious fraud, and (3) accidental fraud.

Malicious fraud is characterized by conscious and deliberate premeditation, aimed at obtaining economic/personal gain through the intentional manipulation of financial statements; acts that involve a high degree of sophistication and a strategy aimed at evading internal control mechanisms or external audits. Notable cases include inflating assets, recording fictitious income, or postponing the disclosure of liabilities, which are deliberate techniques used to project a financial image that is more solid than it really is (Al-Harrasi et al., 2023; Jiang, 2022; Onwubiko, 2020; Zhang et al., 2018).

In contrast, non-malicious fraud is conducted knowingly, that is, it has a different motivation (it responds to ends considered socially acceptable by those who commit it), such as in the case of so-called "Robin Hood fraud," in which employees manipulate figures in the belief that they are helping the organization, their colleagues, or the public good (Al-Harrasi et al., 2023; Jiang, 2022; Onwubiko, 2020; Zhang et al., 2018). Despite this altruistic motivation, these acts constitute a serious ethical and legal violation and distort the fair presentation of financial information.

On the other hand, accidental fraud does not involve fraudulent intent per se, as it stems from errors, negligence, or technical ignorance when internal controls are weak and/or non-existent. It also has detrimental effects on financial statements and poses challenges for auditors faced with the anomaly, who must determine whether these are random errors or recurring behavior that warrants a reassessment of the control environment (Al-Harrasi et al., 2023; Jiang, 2022; Onwubiko, 2020; Zhang et al., 2018).

Accordingly, intent is the driving force behind fraudulent acts and is the ultimate motivation that pushes individuals to deviate from regulatory, ethical, or legal frameworks to obtain undue benefits (Marquart & Thompson, 2024; Narsa et al., 2023). From a criminological and accounting perspective, three main intentions are identified: (1) improving the financial image of the entity; (2) the motivation of the fraudster; and (3) reducing tax or fiscal obligations. These respond to an organizational logic in which the company or those who run it become the subject that decides to manipulate information to achieve certain strategic goals.

First, the intention to improve the entity's financial image occurs when perpetrators deliberately alter financial statements to show a more favorable economic situation than exists. Typical causes include achieving profitability or growth targets imposed by senior management/investors, obtaining financing on more advantageous terms, inflating the market value of shares (stock market fraud), avoiding violations of financial covenants with creditors, and increasing personal bonuses/incentives linked to financial performance (Narsa et al., 2023; Onwubiko, 2020; Parlindungan et al., 2017). In this case, perpetrators seek to present inflated financial statements to project an image of economic strength, operational efficiency, and profitability. They often construct an illusory financial narrative to justify strategic decisions, mergers, acquisitions, or simply the permanence of senior management in their positions (de Oliveira Orth et al., 2024; Murphy & Dacin, 2011; Naldo & Widuri, 2023).

Another view is that fraud is not perpetrated by the company as the agent of fraud, but rather involves individual actors such as employees, managers, or even third parties outside the organization who act to harm or take advantage of it (Dellaportas, 2013; Narsa et al., 2023; Onwubiko, 2020). Nevertheless, an employee who covers up personal embezzlement, a supplier who falsifies documents to overcharge, or a former employee who sabotages accounting systems after a conflict are responding to personal motivations. When analyzing fraud, a distinction is made between corporate and individual/external intent, as each pose quite different risks, consequences, and methods of detection (Narsa et al., 2023; Onwubiko, 2020; Parlindungan et al., 2017).

On the other hand, the intention to reduce tax liability consists of minimizing the tax base by manipulating income, costs, or deductions; this is common in environments where there is a heavy tax burden and weak enforcement (Hudayati et al., 2022; Sarkar & Spieler, 2020; Van Driel, 2019). It includes practices such as: under-reporting actual income, generating fictitious or inflated expenses, using shell companies or false invoicing, manipulating inventories to distort the cost of sales, structuring tax operations to hide income, which affects the company itself and the tax authorities, and by extension society by reducing the state's revenue-raising capacity (Sawangarrearak & Thanathamthee, 2021; Shi et al., 2017; Zhao et al., 2024).

Following on from the above, these intentions reveal an instrumental conception of accounting and a deliberate desire to manipulate information for specific purposes, which constitutes a serious violation of the ethical and legal principles governing business activity (Aboud & Robinson, 2022; De La Torre Lascano & Quiroz, 2023; Nasir et al., 2019). In this approach, accounting records cease to be a neutral and objective reflection of financial

figures and become a strategic resource for the purpose of persuasion/concealment, which leads to altered accounting policies and inaccurate disclosures.

Parallel to intent is persistence, which refers to the temporary and repetitive nature of the fraudulent act, i.e., whether it manifests itself as an isolated event or a continuous pattern over time; this characteristic influences the assessment of cumulative impact, the probability of detection, and the prevention/control mechanisms required in forensic auditing (Leistedt & Linkowski, 2016; Onwubiko, 2020; Raudha & Saeedi, 2019). Accordingly, two types of persistence are established: (1) transient fraud; and (2) permanent fraud. Transient frauds are those that occur only once or sporadically without a pattern of repetition, motivated by immediate needs and circumstantial situations (pressure to close the fiscal year, meet quarterly goals, temporary liquidity crises, etc.). Although their duration is limited, they have a significant impact if they affect key items or coincide with critical moments such as audits or processes to obtain external financing (Al-Harrasi et al., 2023; Jiang, 2022; Onwubiko, 2020).

In contrast to permanent or recurring fraud—which is structurally embedded within the organization's regular processes, making it difficult to detect through standard auditing procedures—cases such as account appropriation, systematic use of fictitious suppliers, and continuous overvaluation of assets illustrate fraud schemes that, once implemented, allow the fraudster to exploit the system continuously until identified, and their detection requires specialized audits, time series review, financial behavior analysis, and in many cases, data mining and ML techniques (Nigro, 2025; Rao & Mandhala, 2024; Raudha & Saeedi, 2019).

Derived from the above, the fraudster's capacity represents the degree of technical skill, access to resources, and understanding of the financial and technological environment on the part of the perpetrator who carries out the fraud; a variable that is underestimated when assessing the level of risk associated with potential fraud and when designing appropriate controls based on the threat profile (Bar Lev et al., 2022; Krokoszinski et al., 2018; Mandal & S., 2024; Onwubiko, 2020). From a structural perspective, it is classified into three levels: minimal, competent, and significant. A fraudster with minimal capability has limited skills and relies on system errors, fortuitous opportunities, or prefabricated tools obtained from third parties (Deep Web). This profile corresponds to low-level employees with access to critical functions but without in-depth technical knowledge. Although their potential for harm is low, their actions in environments with poor controls are risky (Fang et al., 2021; Krokoszinski et al., 2018; Mandal & S., 2024; Uygur & Napier, 2024).

The competence level represents individuals with technical training, professional experience in finance or systems, and a solid understanding of internal processes and organizational vulnerabilities. These actors design more complex frauds such as accounting manipulation, use of offshore structures, or exploitation of legal loopholes, and usually hold positions of trust as accountants, internal auditors, or ERP system managers (Jiang, 2022; Krokoszinski et al., 2018; Zhang et al., 2018).

Finally, fraudsters with significant capabilities are highly meticulous and include organized groups, transnational criminal networks, or even nations; actors who possess advanced skills in cybersecurity and financial analysis and have the technological, human, and financial resources to carry out large-scale, long-term fraud, as well as attacks on accounting systems, corporate identity theft, and infiltration of automated accounting processes, among others. The presence of this threat requires multi-layered controls, continuous audits, and robust cybersecurity frameworks (Dellaportas, 2013; Gray & Debreceeny, 2014; Parlindungan et al., 2017; Villaescusa & Amat, 2022).

Under this premise, the capacity of the fraudster is related to the entity executing the fraud, and refers to the nature of the actor carrying out the fraudulent act, including

the individual and the technology, with implications for detection methods, attribution of responsibility, and corrective/legal actions (Nigro, 2025; Onwubiko, 2020; Raudha & Saeedi, 2019). Traditionally, fraud analysis has focused on individuals, but advances in digitization and automation require a new classification that considers emerging technologies (Brasel et al., 2016; Mandal & S., 2025; Ocampo, 2023; Rashid et al., 2023).

On the one hand, individuals are the most common perpetrators of financial fraud, acting alone or in collusion, and their knowledge of internal systems allows them to exploit weaknesses in controls, accounting policies, or approval processes. However, the growing integration of technology into accounting processes has given rise to new perpetrators of automation who execute, supply, or cover up fraud (Dewi et al., 2024; Erazo-Castillo & De la A-Muñoz, 2023; Leal et al., 2020; Ocampo, 2023; Zambrano Vargas, 2017).

That said, these automated entities include bots, programmed scripts, RPAs (robotic process automation), and specialized malware. Therefore, accurate classification of the executing entity is essential to understanding the perpetration of fraud and appropriate control and defense mechanisms (code auditing, monitoring of automatic processes, cross-validation between human and automated systems), since the presence of automated actors poses challenges in terms of technological governance, traceability, and legal responsibility (Nazarova et al., 2020; Ocampo, 2023; Ramos et al., 2022; Wan-Hussin et al., 2021).

In summary, the intentional dimension requires understanding the type of intent of the fraudster (malicious, non-malicious, or accidental), which is intertwined with personal, institutional, or circumstantial motivation, conditioning the way in which fraud is designed, executed, and justified within the organizational environment. In turn, the persistence of fraud (transitory or permanent) distinguishes between isolated events and systematic schemes that become institutionalized in the entity's financial culture, a dynamic that is exacerbated by the level of the fraudster's ability, which ranges from low, medium, and high skill, capable of circumventing controls; and the executing entity (human or automated—bots, scripts, RPA, or malware), which introduces a technical complexity that challenges traditional audit and internal control models, requiring multidisciplinary approaches that integrate accounting, cybersecurity, and technology governance.

4.1.2. Second Category: Execution of Fraud—Dimension: Method

The execution of fraud is addressed by analyzing the methods used to manipulate financial statements, including recurring fraudulent tactics, schemes, or practices such as altering records, falsifying documents, or using complex corporate structures to cover up illegal operations. Therefore, understanding the methods opens the door to the construction of detection models based on anomalous patterns and the development of more effective forensic audits.

In the field of forensic auditing and corporate financial control, identifying and analyzing the variables that constitute fraud is essential to understanding its evolution and impact on financial statements. Elements such as the method, channel of execution, and accounting/regulatory standards violated impact the information disclosed, which are critical dimensions for diagnosing the risk of material fraud. Each variable reveals the operational mechanics of the fraudulent act and failures in governance, internal control, and regulatory oversight that condone its occurrence. The complexity of the typology of fraud in financial statements requires a systemic approach that integrates regulatory knowledge (IFRS, SOX, GAAP), accounting analysis tools, and professional skepticism criteria in accordance with ISA 240 (IAASB, 2025), in order to ensure the integrity of financial information and the protection of the public interest (Figure 4).

Characteristic	Accounting Manipulation	Document Forgery	Omission of Information
 Technique Used	Alter financial figures	Tamper with documents	Fail to declare elements
 Channel	Any	Any	Any
 Standards Violated	IFRS, GAAP, SOX	Any	IFRS, GAAP, SOX
 Impact on Statements	Distorts financial statements	Distorts financial statements	Distorts financial statements

Figure 4. Contributing variables in the technical dimension of fraud. Source: Authors.

To begin with, the method refers to the specific operating mechanism used to conduct fraud; it classifies fraud based on the materialization of the malicious conduct (DeZoort & Harrison, 2018; Encalada, 2023; Nazarova et al., 2020). The choice of technique is conditioned by the perpetrator's accounting knowledge and their level of access to the organizations' internal systems. Fraudulent techniques include: (1) manipulation of accounting records; (2) falsification or fabrication of documents; and (3) deliberate omission of information.

Given the above, accounting fraud involves distorting, concealing, or altering accounting data and includes: inappropriate changes in accounting policies (modifying the depreciation method without technical justification); early recognition of revenue (before meeting the conditions for accrual); capitalization of current expenses to inflate assets; and not accounting for provisions for asset impairment (Anning & Adusei, 2022; Nyakarimi, 2022; Sequeira et al., 2024). This method requires technical accounting knowledge and is therefore usually perpetrated by personnel with accounting/financial training.

Likewise, the falsification or fabrication of documents corresponds to the creation or modification of documents: false or duplicate invoices, retroactively modified contracts, altered bank statements, falsified audit reports; a method that conceals non-existent transactions or legitimizes fictitious transactions (Hudayati et al., 2022; Naldo & Widuri, 2023; Van Driel, 2019). For its part, the deliberate omission of information on liabilities constitutes a form of fraud, which includes: not disclosing contingent liabilities, omitting post-closing events that affect the financial position; failing to report transactions between related parties; and evading the disclosure of significant financial risks (Gui et al., 2024; P. Lu et al., 2024; Musfi & Soemantri, 2024). Omission in financial figures is complex to detect (more so than falsification) as it is based on the absence of information.

From a forensic audit perspective, the channel represents the operational vector through which the fraudulent act is conducted, constituting a critical variable for the detection, classification, and mitigation of risk. There are digital channels (web, mobile, telephony, IP) that operate within interconnected technological infrastructures, and physical channels referring to manual flows of documents, transactions, and handling of printed accounting media. Each channel has a different attack surface and exposure in terms of internal control and traceability (Ashtiani & Raahemi, 2022; Gray & Debreceeny, 2014; Hogan et al., 2008; Onwubiko, 2020).

In digital channels, fraud takes the form of unauthorized access to ERP systems, alteration of accounting records in databases, manipulation of accounting parameters through backdoors, automation of fictitious transactions with scripts, and orchestration of fraud by unauthorized bots or RPAs. It is facilitated in technological architectures without segrega-

tion of duties, lacking robust authentication or continuous auditing (Gray & Debreceeny, 2014; Rao & Mandhala, 2024; Raudha & Saeedi, 2019; Whiting et al., 2012). In contrast, physical channels provide opportunities for fraud based on document forgery, the use of fraudulent invoices, alteration of manual inventories, and destruction of evidence (Föhr et al., 2025; Gray & Debreceeny, 2014; Onwubiko, 2020). Channel assessment is integrated into audit planning through substantive testing and analytical procedures, considering the materiality of the channel and the level of exposure to information technology (IT) risk in accordance with ISA 315 (IAASB, 2019) and ISO 27001 (ISO & IEC, 2022).

However, financial fraud is legally defined as the intentional violation of accounting principles, regulatory provisions/standards, including International Financial Reporting Standards (IFRS), Generally Accepted Accounting Principles (GAAP), as well as control frameworks such as the Sarbanes-Oxley Act (SOX) and national and local tax laws (Flesher et al., 2018; Imhanzenobe, 2022; Tawiah & Gyapong, 2023; Yassine et al., 2024). Therefore, violation of the standards directly affects the integrity, comparability, and reliability of the accounting information presented to external users, violating the principle of true and fair view (Benkraiem et al., 2022; Johri, 2024; Robles Quiñónez et al., 2024), causing stakeholders to make erroneous decisions due to the alteration of financial information.

Following on from the above, the improper recognition of deferred income contravenes IFRS 15 (García et al., 2023), while the omission of provisions or contingent liabilities violates the provisions of IAS 37, and manipulations in the valuation of intangible assets without economic backing violate IAS 38 and the principles of prudence and consistency (Laguna & Romero, 2009). From the SOX perspective, fraud is defined as material error and failure to certify internal controls by senior management (section 302), in addition to document falsification or destruction of financial evidence (section 802) (Davis et al., 2023; Nazarova et al., 2020). Therefore, forensic auditing documents all regulatory deviations, quantifies the material impact, and issues findings in line with ISA 240, which requires the auditor to critically evaluate professional skepticism when there is a risk of fraud (Ocampo, 2023; Ramos et al., 2022; Tawiah & Gyapong, 2023; Yassine et al., 2024).

The impact of fraud on financial statements translates into a structural alteration of the entity's economic representation, affecting key performance indicators, financial position, and cash flows (Chen et al., 2020; Zajmi, 2019). From a technical point of view, this impact manifests itself as a deliberate overstatement of assets/income, an understatement of liabilities/expenses, and a material omission of post-closing events (in accordance with IAS 10), distorting the judgment of users and infringes on the principles of relevance and fair presentation established in IFRS (Ashtiani & Raahemi, 2022; Blanco et al., 2023; Hogan et al., 2008; Imhanzenobe, 2022).

Thus, typical practices include improper capitalization of operating costs, manipulation of provisions (cookie jar reserves), use of special purpose entities to hide debts off the balance sheet, or use of earnings management techniques to smooth results, actions that negatively impact the quality of accounting information, reduce its usefulness for decision-making, and induce material errors in financial indicators such as EBITDA, ROA, or the debt-to-asset ratio (Andersson & Hellman, 2020; Black et al., 2021; Nyakarimi, 2022; Onwubiko, 2020).

From a forensic perspective, impact assessment must go beyond traditional financial analysis, incorporating vertical and horizontal analysis, specific substantive testing, and the use of data analysis tools to identify anomalous patterns (Kranacher & Riley, 2019; Leal et al., 2020; Nigro, 2025; Ocampo, 2023). In this sense, a professional judgment is made considering whether the impact constitutes intentional manipulation, an accounting error, or a fraudulent omission, categorizing the event as accounting fraud in accordance

with the established COSO and ACFE internal control frameworks (Erazo-Castillo & De la A-Muñoz, 2023; Leal et al., 2020; Rodríguez Salinas, 2023; Zambrano Vargas, 2017).

Therefore, the technical study of variables related to the method, channel of perpetration, violation of accounting standards, and direct effect on financial statements allows for the construction of a risk map for the timely detection of financial fraud. These approaches reinforce the forensic auditor's ability to assess the reasonableness of reported figures and strengthen the design of mitigation strategies within the COSO-based internal control framework. Additionally, recognizing the materialization of fraud through digital manipulation, physical falsification, or aggressive accounting practices, and understanding the violated regulations, is essential for making informed judgments about the existence of intentional material errors. Therefore, the combination of regulatory analysis, document traceability, and advanced analytical procedures is a cornerstone of effective auditing and a coherent institutional response to acts of fraud in financial statements.

4.1.3. Third Category: Participation—Dimension: Level of Collusion

Participation refers to the way in which internal or external actors participate in committing fraud; its collusion dimension studies illicit cooperation between multiple individuals or organizational units to circumvent controls and cover up irregularities. This helps to gauge the magnitude of the risks, given that collusion increases the complexity of detection and weakens conventional oversight systems.

Identifying the source of fraud and the roles involved is essential in forensic auditing and financial control. Figure 5 distinguishes between the level of collusion, internal and external fraud, and analyzes the involvement of managers, auditors, and operators. This involves understanding the structural weaknesses of the internal control system and anticipating risks that affect the integrity of financial statements (Leal et al., 2020; Lee, 2024; Majeed et al., 2023; Ocampo, 2023; Onwubiko, 2020).

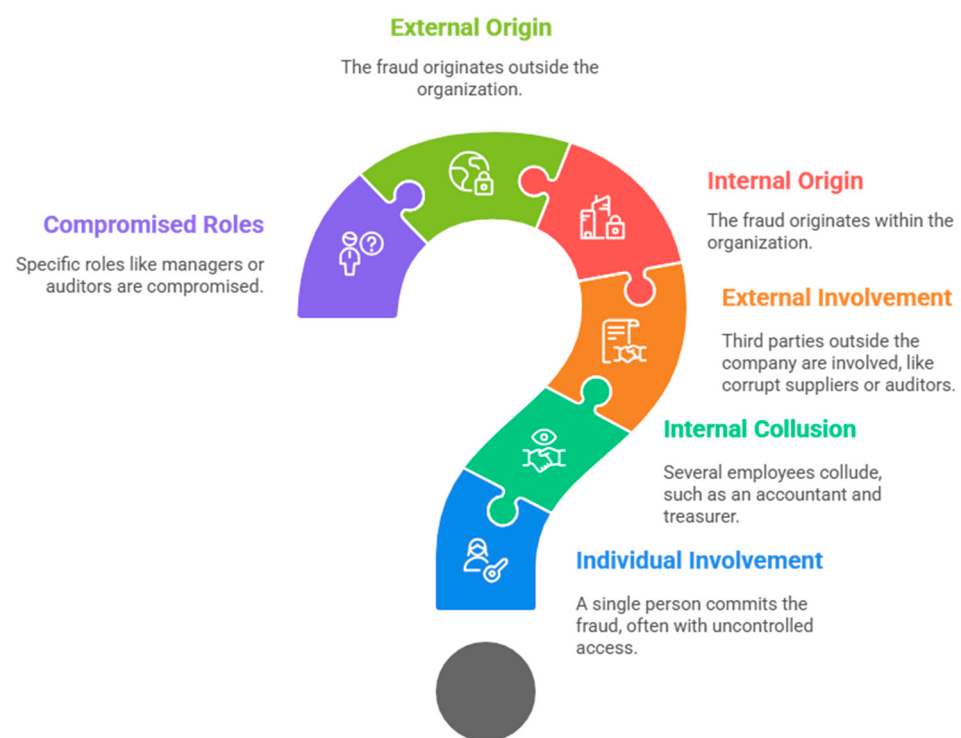


Figure 5. Contributing variables in the participatory dimension of fraud. Source: Authors.

To begin with, the level of collusion refers to the number and type of people involved in committing fraud; this is determined by the degree of sophistication of the fraudulent

scheme and its ability to evade controls: (1) individual fraud; (2) internal collusion; and (3) external collusion. Individual fraud is perpetrated by a single person, usually with privileged access or incompatible functions (who records and approves a transaction); it is usually on a smaller scale, but no less serious (Hagen & Malisa, 2022; Leistedt & Linkowski, 2016; Onwubiko, 2020). This fraud occurs when there is no adequate segregation of duties and, therefore, a single person performs distinct functions.

Likewise, internal collusion involves multiple employees working together to circumvent internal controls. The most common schemes include division of fraud between areas and/or departments (accounting and treasury), supervisors who protect involved subordinates, entire departments committed to fraud, which makes detection complex (Burlando & Motta, 2015; Liu et al., 2023; Villaescusa & Amat, 2022).

External collusion occurs when there is cooperation between employees and external factors such as suppliers, customers, external auditors, or even tax authorities. Common cases include collusion with suppliers to inflate prices, illegal payments in exchange for tax favors, and the use of representatives or shell companies, resulting in highly organized fraud with greater potential for reputational damage (Achmad et al., 2022; Shi et al., 2017; Villaescusa & Amat, 2022).

From an organizational risk management perspective, the system boundary is a key variable for classifying the origin of fraud according to its source: internal or external. On the one hand, internal fraud originates within the structural and functional limits of the entity and involves employees, managers, or personnel with authorized access to accounting and financial systems. This is a serious type of fraud due to the perpetrators' knowledge of internal controls, accounting processes, and weaknesses in the control environment, enabling the manipulation of financial records, the deliberate omission of relevant information, and the misappropriation of assets (Donelson et al., 2017; Nonnenmacher & Marx Gómez, 2021; Onwubiko, 2020; Shi et al., 2017).

On the other hand, external fraud is carried out by actors outside the organization, such as suppliers, customers, hackers, or organized criminal entities, who exploit technological vulnerabilities, contractual loopholes, and deficiencies in access and monitoring controls (Donelson et al., 2017; Nonnenmacher & Marx Gómez, 2021; Onwubiko, 2020; Shi et al., 2017). In both cases, understanding the source of fraud requires the auditor to implement specific evaluation procedures, segment the analysis of inherent risk, and design targeted substantive tests in accordance with ISA 240 and control frameworks such as COSO-ERM and COBIT when digital platforms are involved (Blanco et al., 2023; El-Halaby et al., 2021; Imhanzenobe, 2022; Yassine et al., 2024).

Identifying the functional roles involved in committing fraud is essential in forensic investigation and in mapping responsibilities in the internal control environment (Leal et al., 2020; Rodríguez Salinas, 2023; Zambrano Vargas, 2017). At the same time, the actors involved are classified into three levels: managers, internal/external auditors, and operators or line staff. In this vein, executives, including senior management and corporate governance, commit fraud through strategic decisions that manipulate financial statements in order to achieve performance goals, obtain performance-related financial incentives, or secure access to external financing, thereby committing intentional misrepresentation fraud (Lee, 2024; Majeed et al., 2023; Masulis & Mobbs, 2023).

The involvement of auditors, although less frequent, is critical as it compromises professional independence and leads to systemic failures in oversight; the omission of findings, the concealment of irregularities, and the issuance of opinions without sufficient evidence constitute serious violations of IFAC principles and the Code of Ethics for Professional Accountants (IESBA) (Elsayed et al., 2023; Lisic et al., 2015; Nazarova et al., 2020; Tawiah & Gyapong, 2023). For their part, accounting/administrative operators, being directly

involved in the daily execution of financial processes, manipulate accounting records, falsify source documents, or collaborate in collusion schemes to cover up deviations. Consequently, forensic auditing incorporates transactional analysis techniques, structured interviews, and cross-document testing to determine the participation and responsibility of each role, ensuring a comprehensive, evidence-based approach (Encalada, 2023; Leal et al., 2020; Ocampo, 2023; Rodríguez Salinas, 2023; Zambrano Vargas, 2017).

Ultimately, understanding the duality between the systemic origin of fraud (internal, external), the levels of collusion, and the functional roles involved, enables forensic audit and accounting professionals to develop robust and specific approaches for detecting, preventing, and punishing fraud in financial statements. Therefore, identifying the starting point of the fraud and the hierarchical/technical level of those who execute it provides a way to track recurring patterns and enables the formulation of anti-fraud policies, a more robust governance structure, and differentiated controls according to the degree of risk. This approach is based on forensic analysis methodologies and recognized regulatory frameworks (Gray & Debreceeny, 2014; Onwubiko, 2020), which reinforces the credibility of financial statements and builds an ethical, transparent, and resilient organizational culture in the face of participatory threats.

4.1.4. Fourth Category: Organizational Impact—Dimension: Affected Area

The organizational impact considers the direct and indirect consequences of fraud within the corporate structure; the size of the affected area, the departments, processes, or resources compromised by fraudulent practices, assessing the magnitude of the economic, reputational, and operational damage. Thus, analyzing this relationship allows for the design of targeted mitigation responses and the strengthening of corporate governance policies (Figure 6).

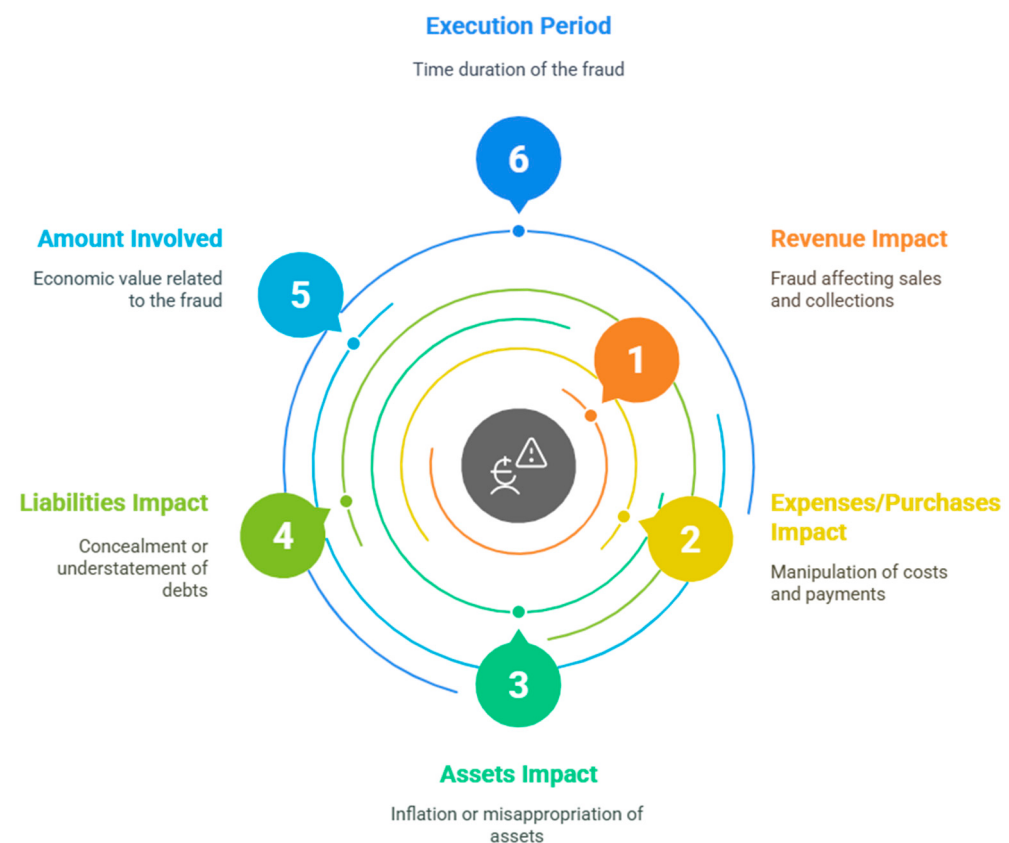


Figure 6. Contributing variables in the operational dimension of fraud. Source: Authors.

Within the analysis of fraud in financial statements, variables related to the type of impact, amount involved, and period of execution represent key dimensions for determining the severity of the offense, the accounting impact, and the efficiency of internal control. These variables define the economic scope of fraud, assess its materiality, and establish timelines to guide the investigation and formulation of findings, with the aim of providing input for the design of institutional, corrective, and preventive responses.

Another key variable is the functional area where fraud occurs, which is classified in terms of its impact on financial statements or operational processes (Musfi & Soemantri, 2024; Onwubiko, 2020; Parlindungan et al., 2017). This dimension includes: (1) revenue fraud, (2) expense and purchasing fraud, (3) asset fraud, and (4) liability fraud.

First, revenue fraud involves the recognition of unrealized revenue, double billing, manipulation of credit sales, and unrecorded returns, which directly affects the income statement and/or profits and is often motivated by pressure to meet sales targets (Błaszczyszński et al., 2021; Phong et al., 2024; Yang, 2022). On the other hand, expense and purchasing fraud manifests itself in the recording of invoices for services not rendered, payments to fictitious suppliers, use of personal/corporate expenses, and increased costs to reduce taxes; it is common in the areas of procurement, logistics, or administration (Hoberg & Lewis, 2017; Mann, 2013; Tan et al., 2024).

At the same time, asset fraud involves the overvaluation of fixed assets, failure to record impairment, non-existent or inflated inventories, and theft of assets (physical fraud). This fraud distorts the balance sheet (statement of financial position) and affects indicators such as ROA and working capital (Nia & Said, 2015; Setiawan & Soewarno, 2025; Souvenir et al., 2025). Finally, liability fraud is the concealment of debts, underestimation of legal provisions, and failure to account for contractual obligations, presenting the company as more solvent than it really is (Demetriades & Owusu-Agyei, 2022; W. Lu & Zhao, 2021; Reurink, 2018).

The analysis of the amount involved in a fraud scheme in the financial statements determines the magnitude of the economic impact on the financial statements and conditions the level of materiality of the irregular event. In auditing, the amount is directly proportional to the risk of detection and the relevance to the auditor's opinion, implying high amounts, accounting distortion, and affecting indicators such as profitability, leverage, and liquidity, misleading external users of the financial statements, including investors, regulatory entities, or banks.

On the contrary, small or moderate frauds, even if they do not individually exceed quantitative thresholds, reflect systematic patterns of illegal behavior. the forensic auditor applies specific procedures such as targeted substantive testing, detailed analytical reviews, and transactional data modeling to identify economic anomalies, focusing on items split into small values that result in significant losses, and the assessment of the amount considers the context of internal control, as weak systems increase the likelihood of fraud.

The period of execution of the fraud, understood as the length of time during which the fraudulent conduct takes place, is another component in the assessment of fraud detection; a variable that distinguishes between short, prolonged, or even chronic fraud, depending on the duration and recurrence of the act (Hogan et al., 2008; Onwubiko, 2020; Rezaee, 2005). In practice, short-term frauds tend to respond to fortuitous opportunities, errors in temporary controls, or occasional unauthorized access; However, prolonged and chronic fraud reveals systematic flaws in the design and operation of internal controls and is often related to collusion structures, repeated misappropriation, and sustained accounting manipulation over time, early recognition of revenue, and prolonged omission of contingent liabilities (Ashtiani & Raahemi, 2022; Burlando & Motta, 2015; Gray & Debreceeny, 2014; Hogan et al., 2008; Villaescusa & Amat, 2022).

As explained above, when the execution period spans several fiscal years, there is a high probability that fraud has contaminated strategic decisions, affected previous audits, and compromised the professional judgment of various levels of supervision. Hence, the forensic auditor analyzes historical trends, applies time series techniques, validates documentation in different fiscal periods, and verifies unusual changes in accounting policies, as these measures function as catalysts for ongoing fraud. Correct identification of the execution period quantifies the cumulative monetary impact and establishes organizational responsibilities and weaknesses over time.

The study of the type of impact, amount involved, and duration of the fraud reveals an interaction of repetitive behavior patterns, prolonged collusion, and structural deficiencies in the internal control architecture. From an accounting perspective, these variables estimate the economic damage and assess the intentionality, sophistication, and systemic risk of the fraud, and their analysis is an integral part of any forensic audit as a basis for informed decision-making, the delimitation of responsibilities, and the implementation of more robust governance mechanisms.

4.1.5. Fifth Category: Environment and Signs—Dimension: Context

The environment and signals category analyzes the context in which fraud is perpetrated and the signs that anticipate its occurrence. Its contextual dimension studies external and internal factors such as regulatory weaknesses, economic pressures, gaps in organizational culture, and atypical behavior patterns. Therefore, identifying these early warning signs is essential for the implementation of predictive monitoring systems and the integration of AI technologies that reinforce the initiative-taking detection of irregularities.

The analysis of the contextual environment leads to the identification of variables such as organizational context, warning indicators, and operational context, which are important in the early detection and assessment of risk in financial statement fraud. These variables help forensic auditors and accounting professionals interpret signs of irregularities and understand the structural/environmental pressures that favor the occurrence of illegal acts. Studying them enriches risk-based auditing and reinforces the effectiveness of internal control systems and the design of preventive strategies.

Although less tangible, the organizational context is a factor in understanding the origins of fraud; Variables such as culture and control (leadership style, reward system, pressure for results, or weak internal control), warning indicators, and operational context create an environment conducive to fraud (Brasel et al., 2016; Encalada, 2023; Nazarova et al., 2020). Similarly, cultural tolerance leads to corruption, inadequate control structures, lack of board oversight, absence of effective reporting channels, and internal audits without independence; factors that influence fraud risk levels (DeZoort & Harrison, 2018; Lisic et al., 2015; Malau et al., 2021).

Warning indicators are symptomatic elements that detect fraud schemes in financial statements at an early stage, quantitative or qualitative signs and deviations from normal patterns and anomalies in accounting and operational processes. Among the most frequent are repeated changes in auditing firms or the company's accountant, suggesting a deliberate attempt to conceal irregularities; inconsistencies in accounting records (recurring errors in bank reconciliations, unusual adjustments at year-end); significant differences between projections and actual results without adequate justification; and lack of supporting documentation for transactions.

Although indicators alone do not prove the existence of fraud, they are red flags that justify the application of extended audit procedures such as reviews of atypical transactions, targeted substantive tests, and structured interviews with key personnel. Therefore, the detection and systematization of these signs, supported by techniques such as financial

data analysis, accounting regression models, and the use of specialized audit software, strengthens the capacity for preventive response to risks of financial information manipulation. Likewise, the operating context is a critical variable in assessing fraud risk, as it encompasses external and internal pressures, structural weaknesses in the organizational environment, and the ethical culture of the entity. Situations such as economic crises, excessive pressure to achieve financial goals, high staff turnover in key areas, and poor oversight by corporate governance create an environment prone to fraud.

According to the fraud triangle theory, the operational context acts as the pressure element that drives certain individuals to rationalize dishonest behavior, especially if it coexists with opportunities and the absence of consequences. The context is reflected in decisions aimed at altering the presentation of financial statements to maintain an image of solvency/profitability before investors, creditors, or regulatory bodies (Dellaportas, 2013; Jiang, 2022; Marquart & Thompson, 2024; Parlindungan et al., 2017).

Considering the above, forensic auditing evaluates the operational context through multidimensional analyses of financial, administrative, corporate governance, and internal control aspects. It involves reviewing board minutes, interviewing compliance officers, evaluating the reporting system, and reviewing the effective implementation of anti-fraud policies. This provides an understanding of the organizational environment and assesses the inherent risk of fraud in order to identify structural factors that must be corrected to mitigate its occurrence (Encalada, 2023; Leal et al., 2020; Ocampo, 2023; Rodríguez Salinas, 2023; Zambrano Vargas, 2017).

Therefore, identifying the organizational context, warning indicators, and operational indicators provides auditors with a basis for supporting their findings and recommendations; these variables function as complementary axes: while the indicators reflect empirical manifestations of accounting deviations, the context conceives the causes linked to cultural, economic, and governance factors. Furthermore, integrating these variables into audit procedures improves the quality of financial reports and strengthens institutional capacity to prevent, detect, and respond to fraud schemes.

4.2. Forensic Framework for the Prevention and Detection of Fraud in Financial Statements

The forensic framework for the prevention and detection of accounting fraud is an analytical and operational tool within the field of forensic auditing and financial criminology; its main objective is to provide a structured, systemic, evidence-based approach to identifying, investigating, and mitigating fraudulent behavior in financial statements (Leal et al., 2020; Ocampo, 2023; Ramos et al., 2022). Therefore, unlike conventional controls, the framework adopts a holistic perspective, integrating accounting, technological, psychological, and organizational elements. This integration is crucial since fraud in financial statements is a multi-causal phenomenon that develops progressively over time, following predictable behavioral and operational patterns, if the appropriate tools are available to detect them (Eutsler et al., 2016; Roszkowska, 2021; Wu et al., 2022).

First, the framework is based on a forensic risk assessment that involves identifying vulnerable areas within accounting and financial processes. It considers traditional critical accounts such as accounts receivable, unearned revenue, or intangible assets, and those areas where accounting judgment is subjective, resulting from high estimates of impairments, provisions, or the valuation of complex financial instruments (Mabelane et al., 2022; Nigrini, 2019; Rodríguez Salinas, 2023). This phase incorporates the analysis of inherent, control, and residual risk, considering organizational control factors, incentives for manipulation, pressure from financial goals, and corporate governance structure (Chen et al., 2020; Ramírez-Alpízar et al., 2020; Suljić et al., 2025). Here, scenario analysis techniques, risk matrices, and quantitative fraud prediction models (Beneish M-Score model or logistic

regression on financial ratios) are applied (DeZoort & Harrison, 2018; Kim et al., 2016; W. Lu & Zhao, 2021).

Next, the framework includes a set of preventive controls of a forensic nature, designed to comply with regulatory requirements and anticipate fraudulent behavior before it occurs (Baumgärtler et al., 2024; Cugniere et al., 2022; Onwubiko, 2020). These include the implementation of clear and restrictive policies regarding unusual transactions, the segregation of duties, especially in the income, payment, and accounting closing cycles, and the limitation of access to ERP systems (Bhattacharya & Mickovic, 2024; Leistedt & Linkowski, 2016; Musfi & Soemantri, 2024). At this stage, emphasis is placed on the development of early warnings based on accounting rules and exception algorithms, which approve the stopping of processes in real time when statistical deviations from historical or budgetary parameters are detected (de Oliveira Orth et al., 2024; Gupta & Mehta, 2021; Hamza et al., 2023).

The third dimension of the framework is continuous monitoring and digital forensic auditing, a critical phase that represents the modern evolution of the traditional sampling-based approach; Computer-assisted audit tools (CAATs), data mining, and predictive analytics are used, enabling forensic investigators to track millions of accounting records in search of anomalous patterns, round transactions, inconsistent consolidations, covert duplications, and off-hour movements or movements with suspicious counterparties (DeZoort & Harrison, 2018; Malau et al., 2021; Ocampo, 2023). Thus, AI models such as artificial neural networks, support vector machines (SVM), and unsupervised clustering algorithms (K-means) are incorporated to identify atypical behavior, even when the fraud is designed to appear normal; This stage allows for early detection of fraud and the construction of financial risk profiles by business unit, user, or accounting segment (Eutsler et al., 2016; Leal et al., 2020; Ramos et al., 2022).

Finally, the framework recognizes that no technical measure can be fully effective without an ethical organizational culture that is resilient to fraud; the cultural component is both a risk factor and a control element (Erazo-Castillo & De la A-Muñoz, 2023; Mat Ridzuan et al., 2022; Roszkowska, 2021). Therefore, organizations must promote ethical values through ongoing training on financial integrity, establish anonymous and secure reporting lines, and reinforce transparency at all hierarchical levels (Rodríguez Salinas, 2023; Zemankova, 2019). Additionally, it has been shown that a culture of compliance is built by the example set by senior management and consistency between corporate discourse and daily practices; that culture includes ethical health indicators, organizational climate surveys, and code of conduct compliance audits as an integral part of the anti-fraud ecosystem (Mabelane et al., 2022; Nigrini, 2019; Rodríguez Salinas, 2023).

Thus, the forensic framework for financial statement fraud articulates diverse levels of analysis, from micro accounting control to organizational meta-analysis, for a scientific approach to the phenomenon of financial statement fraud. By combining quantitative techniques with qualitative methods, and advanced technologies with human understanding of the motivations behind fraud, this approach maximizes entities' ability to detect and prevent manipulation that compromises the accuracy and integrity of their financial reports. It becomes a strategic tool that protects the organization's assets and reputation, with the aim of contributing to the strengthening of the financial system and public confidence in accounting information (Achmad et al., 2022; Leistedt & Linkowski, 2016; Onwubiko, 2020; Phong et al., 2024).

5. Conclusions

This analysis shows that corporate fraud is a systemic and adaptable phenomenon fueled by structural weaknesses of internal control, contextual pressures, and technological advances. The article shows that the structure represented in categories, dimensions, and

variables presents in detail elements that reflect an analysis of fraudulent acts, their implicit causes, and how they manifest themselves. Components, such as intention, motivation, and persistence, highlight the causes that trigger fraudulent conduct. Likewise, the analysis of execution methods, their channels, and violated regulations shows that these acts are operationally articulated and as a consequence accounting and financial information is distorted.

The involvement of automated entities (bots, scripts, RPA, or malware) shows new approaches moving from traditional audits to systematized audits, where the origin of fraud with its stages, the security of the system, and the continuous monitoring of automated activities represent great relevance for the supervision of human processes. Thus, the integration of variables related to the impact and the organizational operational context exposes that fraud manifests itself when there is a union between malicious incentives, economic pressures, deficiencies in supervision, and weak organizational culture.

The incorporation of AI-based systems, as a cutting-edge and effective strategy, allows optimizing the detection, prevention, and monitoring of fraudulent activities in financial statements. Through learning models, data mining techniques, and anomaly detection algorithms, AI analyzes volumes of data generated by the company's daily transactions that support accounting records, identifying anomalies, hidden correlations, and manipulation in the figures of accounting reports, which traditional auditing methods fail to detect. The capacity for constant learning and its continuous adaptation allows internal control to be strengthened, which in turn generates a greater organizational culture and solid corporate governance, increasing the trust of stakeholders, with information that ensures the integrity, transparency, and accuracy of the financial information disclosed; essential for the sustainability and durability of laorganizaciones.es.

The framework provides practitioners, researchers, and compliance officers with a common language and a robust conceptual framework that allows for the design of policies, processes, and tools for continuous monitoring. The framework also presents the analysis of how data are collected and processed in forensic investigation, internal auditing, and early warning systems, considering elements such as procedural complexity and ethical and legal restrictions associated with the use of sensitive information.

That said, the categorization presented is a flexible and updatable basis, capable of transforming as methods, fraudulent actors, technologies, and regulatory frameworks change. Its consolidation provides new lines of dialogue between academia, accounting professionals, forensic auditors, and engineers in charge of cybersecurity and corporate governance, based on the formulation of internal policies for comprehensive fraud prevention in interconnected and challenging contexts.

From an interpretative perspective, the findings underscore the relevance of financial sustainability because once fraud has materialized, it causes business instability due to its financial and reputational consequences. Organizations that suffer recurring losses, low liquidity, or deteriorated solvency are under constant pressure to maintain a favorable financial image to minimize any risk of manipulation of financial information, since the consequences would affect organizational continuity and the failure to meet the expectations of stakeholders.

In this sense, the company is threatened to continue its operations and fall into bankruptcy, triggered by the persistence of fraudulent schemes in financial reports. An increase in the probability of organizational failure can distort financial information, specifically in the recognition of income, the concealment of payments, and misleading disclosures. Incorporating financial distress and sustainability information into analysis reinforces the explanatory power of the proposed framework and increases its importance for auditors,

regulators, and accounting professionals looking for early warning signs of manipulation in financial figures.

5.1. Limitations

Despite its conceptual and operational breadth, the proposed framework has limitations due to its descriptive and taxonomic nature. First, the empirical validation of the classification and the accuracy of the subvariables depend on their systematic application in real organizational contexts, which requires access to sensitive data, internal audit processes, and proven cases of fraud, circumstances that are often restricted by corporate confidentiality. Furthermore, although the framework contemplates emerging variables such as automation and the participation of non-human actors, its practical applicability faces technical challenges such as the capacity of accounting and auditing information systems to capture, process, and analyze large volumes of digital records and metadata. Another limitation lies in the possible subjectivity in the categorization of intentions and motivations, given that the interpretation of psychological and cultural factors varies among organizations, auditors, and regulatory environments. Therefore, by focusing on accounting and operational fraud, the framework does not comprehensively address other types of financial fraud, which require complementary frameworks or more robust interdisciplinary approaches.

5.2. Future Work

Given the conceptual and literature-based nature of this study, one of its main limitations lies in the absence of empirical validation. Accordingly, future research should focus on empirically and statistically validating the proposed framework through case studies, longitudinal forensic audits, and comparative analyses across industries and regulatory authorities, to assess the robustness, applicability, and generalizability of each category and analytical dimension.

A second limitation relates to the qualitative and conceptual formulation of the proposed dimensions. To address this, future studies could operationalize the framework by developing quantitative metrics and indicators derived from its classification structure, enabling their integration into expert systems, machine learning algorithms, and automated fraud monitoring dashboards. This would enhance the practical applicability of the framework in auditing and advanced analytics contexts.

Additionally, the framework does not explicitly model dynamic organizational and contextual factors. Future research could therefore explore the interaction between organizational culture, contextual pressures, and the resilience of internal controls, particularly under conditions of intensive digitalization. Mixed methods approach combining qualitative techniques (e.g., interviews and ethnographic studies) with data mining could help overcome this limitation.

Finally, another limitation of the present study is its static perspective on fraud phenomena. Future research should examine how the proposed framework performs under conditions of economic crisis or regulatory change, as such environments may alter fraud patterns and expose new vulnerabilities not captured in the current analysis.

5.3. Management Implications

From a corporate management and governance perspective, the framework provides guidelines for strengthening internal control architecture by identifying vulnerabilities linked to organizational culture, perverse incentives, and deficiencies in oversight. In this way, the operating context variable, in conjunction with warning indicators and system limits, underscores the importance of mapping internal and external pressures arising from fraudulent acts, facilitating preventive interventions such as segregation of duties,

rotation of sensitive positions, and implementation of corporate integrity and ethics policies. Likewise, the classification of organizational impact that distinguishes between income, expenses, assets, and liabilities allows senior management to prioritize audit resources and design mitigation plans proportional to the level of exposure and materiality of the risks detected. It provides input for strategic decision-making on the allocation of monitoring and control resources, the design of incident response protocols, and communication with internal and external stakeholders, strengthening transparency and trust in accountability.

5.4. Practical Implications

The proposed framework represents a methodological tool of high operational value for auditors, forensic consultants, and internal control managers, offering a detailed structure that identifies, classifies, and monitors fraud schemes in a systematic manner. Its breakdown into categories such as intent, motivation, persistence, execution channel, and executing entity makes it possible to design detection and response strategies tailored to the nature of the event, surpassing traditional practices based solely on superficial financial indicators. Thus, the incorporation of non-human actors such as bots, scripts, or malware broadens the scope of the audit to include cybersecurity and automation, integrating the analysis of digital records, traceability of automated processes, and system integrity verification. On the other hand, the consideration of multiple channels and regulatory violations provides access to multi-criteria audits and reinforces the supervision of regulatory compliance under frameworks such as IFRS, GAAP, or SOX. This approach enables the development of early warning systems and control dashboards, optimizing the ability to react to accounting anomalies, which strengthens the traceability of operations to support investigation processes with robust and replicable evidence.

5.5. Theoretical Implications

In theoretical terms, the framework contributes to the literature by expanding classic frameworks such as the Fraud Triangle and its contemporary extensions (Pentagon and Diamond of Fraud) by incorporating variables such as the technical capacity of the fraudster, the temporal persistence of fraud, and the participation of automated entities, aspects that have been little studied. This multilevel approach conceptualizes fraud as a socio-technical and organizational phenomenon, integrating behavioral, structural, and technological dimensions into an analytical framework. Its structure allows for the operationalization of variables for comparative empirical studies across industries, sectors, and diverse regulatory environments, providing a basis for developing metrics, indicators, and predictive models based on pattern analysis and data mining. Therefore, the framework lays the groundwork for new lines of research focused on the resilience of control systems in the face of advanced automation and regulatory complexity, articulating financial auditing, technological risk analysis, and ethical governance as interdependent axes for understanding and mitigating fraud.

Author Contributions: Conceptualization, L.H.A. and J.J.S.M.; methodology, L.H.A.; software, J.J.M.H.; validation, L.H.A., J.J.S.M. and J.J.M.H.; formal analysis, L.H.A.; investigation, J.J.S.M.; resources, J.J.M.H.; data curation, J.J.M.H.; writing—original draft preparation, L.H.A.; writing—review and editing, J.J.S.M. and J.J.M.H.; visualization, J.J.M.H.; supervision, J.J.S.M.; project administration, L.H.A.; funding acquisition, J.J.S.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Universidad Cooperativa de Colombia, grant number INV 3653.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data supporting the findings of this study are available from the corresponding author upon reasonable request.

Acknowledgments: Universidad de La Salle and Universidad Cooperativa de Colombia.

Conflicts of Interest: The authors declare no conflicts of interest.

References

- Aboud, A., & Robinson, B. (2022). Fraudulent financial reporting and data analytics: An explanatory study from Ireland. *Accounting Research Journal*, 35(1), 21–36. [CrossRef]
- ACFE. (2024). *Occupational fraud 2024: A report to the nations*. Available online: <https://www.acfe.com/-/media/files/acfe/pdfs/rtnn/2024/2024-report-to-the-nations.pdf> (accessed on 1 June 2025).
- Achmad, T., Ghozali, I., Helmina, M. R. A., Hapsari, D. I., & Pamungkas, I. D. (2022). Detecting fraudulent financial reporting using the fraud hexagon model: Evidence from the banking sector in Indonesia. *Economies*, 11(1), 5. [CrossRef]
- Al-Harrasi, A., Shaikh, A. K., & Al-Badi, A. (2023). Towards protecting organisations' data by preventing data theft by malicious insiders. *International Journal of Organizational Analysis*, 31(3), 875–888. [CrossRef]
- Andersson, P., & Hellman, N. (2020). Analysts' evaluations of acquisitions: Swedish survey evidence on IFRS knowledge and the use of accounting information for valuation purposes. *Journal of International Accounting, Auditing and Taxation*, 41, 100354. [CrossRef]
- Anning, A. A., & Adusei, M. (2022). An analysis of financial statement manipulation among listed manufacturing and trading firms in Ghana. *Journal of African Business*, 23(1), 165–179. [CrossRef]
- Ashtiani, M. N., & Raahemi, B. (2022). Intelligent fraud detection in financial statements using machine learning and data mining: A systematic literature review. *IEEE Access*, 10, 72504–72525. [CrossRef]
- Bandara, S., & Falta, M. (2021). The usefulness of IFRS-compliant reports: Perceptions of Sri Lankan investors and lenders. *Asian Review of Accounting*, 29(4), 525–557. [CrossRef]
- Bar Lev, E., Maha, L.-G., & Topliceanu, S.-C. (2022). Financial frauds' victim profiles in developing countries. *Frontiers in Psychology*, 13, 999053. [CrossRef] [PubMed]
- Baumgärtler, T., Eudelle, P., & Cano, J. G. (2024). An international analysis of fraud detection in European structural and investment funds. *European Journal of International Management*, 22(2), 198–229. [CrossRef]
- Benkraiem, R., Bensaad, I., & Lakhal, F. (2022). How do international financial reporting standards affect information asymmetry? The importance of the earnings quality channel. *Journal of International Accounting, Auditing and Taxation*, 46, 100445. [CrossRef]
- Bhattacharya, I., & Mickovic, A. (2024). Accounting fraud detection using contextual language learning. *International Journal of Accounting Information Systems*, 53, 100682. [CrossRef]
- Black, D. E., Christensen, T. E., Ciesielski, J. T., & Whipple, B. C. (2021). Non-GAAP earnings: A consistency and comparability crisis? *Contemporary Accounting Research*, 38(3), 1712–1747. [CrossRef]
- Blanco, B., Dhole, S., & Gul, F. A. (2023). Financial statement comparability and accounting fraud. *Journal of Business Finance & Accounting*, 50(7–8), 1166–1205. [CrossRef]
- Błaszczczyński, J., de Almeida Filho, A. T., Matuszyk, A., Szelać, M., & Słowiński, R. (2021). Auto loan fraud detection using dominance-based rough set approach versus machine learning methods. *Expert Systems with Applications*, 163, 113740. [CrossRef]
- Boddy, C. R., Freeman, C., & Karpacheva-Hock, E. (2024). Fraud and corporate psychopaths: The proposition for reintroducing personality traits of the economic crime offender. *Journal of Economic Criminology*, 5, 100081. [CrossRef]
- Brasel, K., Doxey, M. M., Grenier, J. H., & Reffett, A. (2016). Risk disclosure preceding negative outcomes: The effects of reporting critical audit matters on judgments of auditor liability. *The Accounting Review*, 91(5), 1345–1362. [CrossRef]
- Burlando, A., & Motta, A. (2015). Collusion and the organization of the firm. *American Economic Journal: Microeconomics*, 7(3), 54–84. [CrossRef]
- Bustamante, L. X., Hernández Aros, L., & Gutiérrez Portela, F. (2025). Financial fraud detection through the application of machine learning techniques with an anomaly-based approach. In *Human-computer interaction. HCI-COLLAB 2024* (pp. 159–172). Springer. [CrossRef]
- Chen, L., Xiu, B., & Ding, Z. (2020). Finding misstatement accounts in financial statements through ontology reasoning. *IEEE Access*, 13, 124449–124462. [CrossRef]
- Christensen, B. E., Newton, N. J., & Wilkins, M. S. (2024). Costs and benefits of a risk-based PCAOB inspection regime. *Accounting, Organizations and Society*, 112, 101552. [CrossRef]
- Clauss, P., Roncalli, T., & Weisang, G. (2009). Risk management lessons from madoff fraud. In *Credit, currency, or derivatives: Instruments of global financial stability or crisis?* (pp. 505–543). Emerald Group Publishing Limited. [CrossRef]
- Cox, H., & Mowatt, S. (2019). Horatio Bottomley and the rise of John Bull magazine. *Media History*, 25(1), 100–125. [CrossRef]

- Cugniere, A., Tusch, O., & Mösenbacher, A. (2022). How fraud detection technologies can help to detect damages in aircraft structures. *Procedia Structural Integrity*, 38, 168–181. [CrossRef]
- Davis, R. T., Lopez, T. J., & Pollard, T. (2023). The joint influence of Sarbanes-Oxley and FAS123R on financial misreporting. *Journal of Business Finance & Accounting*, 50(9–10), 1836–1866. [CrossRef]
- De La Torre Lascano, C. M., & Quiroz, J. I. (2023). Ciberdelito y su asociación en el cometimiento de fraudes financieros en la pandemia de la COVID-19. *Revista Venezolana de Gerencia*, 28(102), 609–628. [CrossRef]
- Dellaportas, S. (2013). Conversations with inmate accountants: Motivation, opportunity and the fraud triangle. *Accounting Forum*, 37(1), 29–39. [CrossRef]
- Demetriades, P., & Owusu-Agyei, S. (2022). Fraudulent financial reporting: An application of fraud diamond to Toshiba's accounting scandal. *Journal of Financial Crime*, 29(2), 729–763. [CrossRef]
- de Oliveira Orth, C., Momo, F., Manfroi da Silva Bonotto, M., & Schiavi, G. (2024). Motivational processes involved in the behavior of the financial statement fraudster. *Journal of Financial Crime*, 31(6), 1362–1373. [CrossRef]
- Dewi, N. S., Said, J., Faiza, S. N., & Julian, L. (2024). The effect of big data competencies and tone at the top on internal auditors fraud detection effectiveness. *Decision Science Letters*, 13(1), 153–160. [CrossRef]
- DeZoort, F. T., & Harrison, P. D. (2018). Understanding auditors' sense of responsibility for detecting fraud within organizations. *Journal of Business Ethics*, 149(4), 857–874. [CrossRef]
- Dimmock, S. G., & Gerken, W. C. (2011). Finding Bernie Madoff: Detecting fraud by investment managers. *SSRN Electronic Journal*, 1–62. [CrossRef]
- Donelson, D. C., Ege, M. S., & McInnis, J. M. (2017). Internal control weaknesses and financial reporting fraud. *Auditing: A Journal of Practice & Theory*, 36(3), 45–69. [CrossRef]
- El-Halaby, S., Aboul-Dahab, S., & Bin Qoud, N. (2021). A systematic literature review on AAOIFI standards. *Journal of Financial Reporting and Accounting*, 19(2), 133–183. [CrossRef]
- Elsayed, M., Elshandidy, T., & Ahmed, Y. (2023). Is expanded auditor reporting meaningful? UK evidence. *Journal of International Accounting, Auditing and Taxation*, 53, 100582. [CrossRef]
- Encalada, V. R. (2023). Auditoría forense: Riesgo de auditoría, fraude y materialidad. *Suma de Negocios*, 14(31), 122–135. [CrossRef]
- Erazo-Castillo, J., & De la A-Muñoz, S. (2023). Auditoría del futuro, la prospectiva y la inteligencia artificial para anticipar riesgos en las organizaciones. *Novasineria Revista Digital de Ciencia, Ingeniería y Tecnología*, 6(1), 105–119. [CrossRef]
- Eutsler, J., Nickell, E. B., & Robb, S. W. G. (2016). Fraud risk awareness and the likelihood of audit enforcement action. *Accounting Horizons*, 30(3), 379–392. [CrossRef]
- Fang, V. W., Li, N., Wang, W., & Zhang, G. (2021). *Everlasting fraud* (pp. 1–74). European Corporate Governance Institute—Law Working Paper No. 617/2021. Available online: <https://ssrn.com/abstract=3762260> (accessed on 5 December 2025).
- Flesher, D. L., Flesher, T. K., & Previts, G. J. (2018). The financial accounting standards board: Profiles of seven leaders. *Research in Accounting Regulation*, 30(1), 38–48. [CrossRef]
- Föhr, T. L., Reichelt, V., Marten, K.-U., & Eulerich, M. (2025). A framework for the structured implementation of process mining for audit tasks. *International Journal of Accounting Information Systems*, 56, 100727. [CrossRef]
- García, G. H., Hernández Arauz, M. A., Zárate Fonseca, S. E., & Chicaiza Sánchez, O. L. (2023). NIIF 15: Un diagnóstico inicial conforme la norma internacional de información financiera. *Revista Eruditus*, 4(1), 43–57. [CrossRef]
- Gray, G. L., & Debreceeny, R. S. (2014). A taxonomy to guide research on the application of data mining to fraud detection in financial statement audits. *International Journal of Accounting Information Systems*, 15(4), 357–380. [CrossRef]
- Gui, Z., Huang, Y., & Zhao, X. (2024). Financial fraud and investor awareness. *Journal of Economic Behavior & Organization*, 219, 104–123. [CrossRef]
- Gupta, S., & Mehta, S. K. (2021). Data mining-based financial statement fraud detection: Systematic literature review and meta-analysis to estimate data sample mapping of fraudulent companies against non-fraudulent companies. *Global Business Review*, 25, 1290–1313. [CrossRef]
- Hagen, J., & Malisa, A. (2022). Financial fraud and individual investment behavior. *Journal of Economic Behavior & Organization*, 203, 593–626. [CrossRef]
- Hamza, C., Lylia, A., Nadine, C., & Nicolas, C. (2023). Semi-supervised method to detect fraudulent transactions and identify fraud types while minimizing mounting costs. *International Journal of Advanced Computer Science and Applications*, 14(2), 861–870. [CrossRef]
- Hernandez, L., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodríguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. *Humanities and Social Sciences Communications*, 11(1), 1130. [CrossRef]
- Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. *Expert Systems with Applications*, 193, 116429. [CrossRef]
- Hoberg, G., & Lewis, C. (2017). Do fraudulent firms produce abnormal disclosure? *Journal of Corporate Finance*, 43, 58–85. [CrossRef]

- Hogan, C. E., Rezaee, Z., Riley, R. A., & Velury, U. K. (2008). Financial statement fraud: Insights from the academic literature. *Auditing: A Journal of Practice & Theory*, 27(2), 231–252. [CrossRef]
- Hudayati, A., Nisa, T. K., & Sanusi, Z. M. (2022). Financial pressure and related party transactions on financial statement fraud: Fraud triangle perspective. *International Journal of Business and Emerging Markets*, 14(2), 213–230. [CrossRef]
- IAASB. (2019). *ISA 315 (revised 2019): Identifying and assessing the risks of material misstatement* (International Federation of Accountants (IFAC) Ed.). IAASB. Available online: <https://www.iaasb.org/publications/isa-315-revised-2019-identifying-and-assessing-risks-material-misstatement> (accessed on 5 December 2025).
- IAASB. (2025). *ISA 240 (revised): The auditor's responsibilities relating to fraud in an audit of financial statements* (International Federation of Accountants (IFAC) Ed.). IAASB. Available online: <https://www.iaasb.org/publications/isa-240-revised-auditor-s-responsibilities-relating-fraud-audit-financial-statements> (accessed on 5 December 2025).
- International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2022). *ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection—Information security management systems—Requirements* (3rd ed.). Available online: <https://www.iso.org/standard/27001> (accessed on 5 December 2025).
- Imhanzenobe, J. (2022). Value relevance and changes in accounting standards: A review of the IFRS adoption literature. *Cogent Business & Management*, 9(1), 2039057. [CrossRef]
- Jiang, R. (2022). Exploring employees' computer fraud behaviors using the fraud triangle theory. *Pacific Asia Journal of the Association for Information Systems*, 14, 100–121. [CrossRef]
- Johri, A. (2024). Examining the impact of international financial reporting standards adoption on financial reporting quality of multinational companies. *International Journal of Financial Studies*, 12(4), 96. [CrossRef]
- Kim, Y. J., Baik, B., & Cho, S. (2016). Detecting financial misstatements with fraud intention using multi-class cost-sensitive learning. *Expert Systems with Applications*, 62, 32–43. [CrossRef]
- Kranacher, M.-J., & Riley, R. (2019). *Forensic accounting and fraud examination*. John Wiley & Sons. Available online: https://books.google.com.co/books/about/Forensic_Accounting_and_Fraud_Examination.html?id=GnOODwAAQBAJ&redir_esc=y (accessed on 1 June 2025).
- Krokoszinski, L., Westenberger, A., & Hosser, D. (2018). Social competencies and the sociomoral reflectiveness of imprisoned fraudsters. *Journal of Forensic Practice*, 20(4), 279–288. [CrossRef]
- Laguna, J. P., & Romero, E. C. (2009). Las sociedades que utilizan las NIC/NIIF ya no tienen que reconciliar las cifras contables a us gaap. ¿está justificada esta decisión de la sec en el ámbito del sector de las telecomunicaciones? *Revista de Contabilidad*, 12(1), 45–93. [CrossRef]
- Leal, L., Rodríguez, E., & González, R. (2020). Auditoría forense: Los procedimientos del Contador Público en la investigación del fraude corporativo. *Gestión y Sociedad*, 3(2), 141–160.
- Lee, S. (2024). Has R&D investment become riskier for CEOs after the Sarbanes Oxley act? *Journal of Corporate Accounting & Finance*, 35(3), 350–363. [CrossRef]
- Leistedt, S. J., & Linkowski, P. (2016). Fraud, individuals, and networks: A biopsychosocial model of scientific frauds. *Science & Justice*, 56(2), 109–112. [CrossRef] [PubMed]
- Lisic, L. L., Silveri, S. (Dino), Song, Y., & Wang, K. (2015). Accounting fraud, auditing, and the role of government sanctions in China. *Journal of Business Research*, 68(6), 1186–1195. [CrossRef]
- Liu, C., Ryan, D., Lin, G., & Xu, C. (2023). No rose without a thorn: Corporate teamwork culture and financial statement misconduct. *Journal of Behavioral and Experimental Finance*, 37, 100786. [CrossRef]
- Lu, P., Wang, Y., & Li, B. (2024). Short selling and corporate financial fraud: Empirical evidence from China. *International Review of Economics & Finance*, 89, 1569–1582. [CrossRef]
- Lu, W., & Zhao, X. (2021). Research and improvement of fraud identification model of Chinese A-share listed companies based on M-score. *Journal of Financial Crime*, 28(2), 566–579. [CrossRef]
- Mabelane, K., Mongwe, W. T., Mbuva, R., & Marwala, T. (2022). An analysis of local government financial statement audit outcomes in a developing economy using machine learning. *Sustainability*, 15(1), 12. [CrossRef]
- Majeed, M. A., Xie, S., Ullah, I., Fu, J., & Wang, C. (2023). Do powerful CEOs affect qualitative financial disclosure? Evidence from accounting comparability. *Research in International Business and Finance*, 66, 102026. [CrossRef]
- Malau, W. C., Ohalehi, P., Badr, E. S., & Yekini, K. (2021). Fraud interpretation and disclaimer audit opinion. *Managerial Auditing Journal*, 36(2), 240–260. [CrossRef]
- Mandal, A., & S., A. (2024). Fathoming fraud: Unveiling theories, investigating pathways and combating fraud. *Journal of Financial Crime*, 31(5), 1106–1125. [CrossRef]
- Mandal, A., & S., A. (2025). Preventing financial statement fraud in the corporate sector: Insights from auditors. *Journal of Financial Reporting and Accounting*, 23(1), 56–80. [CrossRef]
- Mann, L. (2013). How to reduce the risk of purchasing fraud. *Healthcare Financial Management: Journal of the Healthcare Financial Management Association*, 67(7), 78–82. [PubMed]

- Marquart, J., & Thompson, A. (2024). Exploring relation fraud, murder, and the Fraud Triangle. *Journal of Economic Criminology*, 4, 100061. [\[CrossRef\]](#)
- Masulis, R. W., & Mobbs, S. (2023). Influential independent directors' reputation incentives: Impacts on CEO compensation contracts and financial reporting. *Journal of Corporate Finance*, 82, 102449. [\[CrossRef\]](#)
- Mat Ridzuan, N. I., Said, J., Razali, F. M., Abdul Manan, D. I., & Sulaiman, N. (2022). Examining the role of personality traits, digital technology skills and competency on the effectiveness of fraud risk assessment among external auditors. *Journal of Risk and Financial Management*, 15(11), 536. [\[CrossRef\]](#)
- Mensah, J. M. K. (2012). Why Lehman Brothers failed: "Preventive measures and recommendations". *SSRN Electronic Journal*, 5(4), 85–91. [\[CrossRef\]](#)
- Mohammed, A. (2023). The impact of the fraud examiners on fraud risk management in Lehman Brothers Inc. in the financial crisis in the United States. *International Journal of Research and Studies Publishing*, 4(47), 309–336. [\[CrossRef\]](#)
- Munawar, Z., Yahya, S., & Siti-Nabiha, A. K. (2012). Sell-side security analysts: Re-reporting of Enron corporation fraudulent financial data. *Procedia-Social and Behavioral Sciences*, 62, 749–760. [\[CrossRef\]](#)
- Murphy, P. R., & Dacin, M. T. (2011). Psychological pathways to fraud: Understanding and preventing fraud in organizations. *Journal of Business Ethics*, 101(4), 601–618. [\[CrossRef\]](#)
- Musfi, P. N., & Soemantri, R. (2024). The effect of nature of industry, financial stability, ineffective monitoring, and changes in company directors on indications of fraudulent financial statements. *Indonesian Journal of Economics, Social, and Humanities*, 6(1), 16–37. [\[CrossRef\]](#)
- Naldo, R. R., & Widuri, R. (2023). Fraudulent financial reporting and fraud hexagon: Evidence from infrastructure companies in ASEAN. *Economic Affairs*, 68(3), 1455–1468. [\[CrossRef\]](#)
- Narsa, N., Afifa, L., & Wardhaningrum, O. (2023). Fraud triangle and earnings management based on the modified M-score: A study on manufacturing company in Indonesia. *Heliyon*, 9(2), e13649. [\[CrossRef\]](#)
- Nasir, N. A. B. M., Ali, M. J., & Ahmed, K. (2019). Corporate governance, board ethnicity and financial statement fraud: Evidence from Malaysia. *Accounting Research Journal*, 32(3), 514–531. [\[CrossRef\]](#)
- Nazarova, K., Mysiuk, V., Gordoplov, V., Koval, V., & Danilevičienė, I. (2020). Preventional audit: Implementation of sox control to prevent fraud. *Business: Theory and Practice*, 21(1), 293–301. [\[CrossRef\]](#)
- Nia, E. H., & Said, J. (2015). Assessing fraud risk factors of assets misappropriation: Evidences from Iranian banks. *Procedia Economics and Finance*, 31, 919–924. [\[CrossRef\]](#)
- Nigrini, M. J. (2019). The patterns of the numbers used in occupational fraud schemes. *Managerial Auditing Journal*, 34(5), 606–626. [\[CrossRef\]](#)
- Nigro, H. (2025). Contabilidad forense digital: Nuevas herramientas para la detección del fraude financiero. *Revista Colombiana de Contabilidad*, 13(26), 37–57. [\[CrossRef\]](#)
- Nonnenmacher, J., & Marx Gómez, J. (2021). Unsupervised anomaly detection for internal auditing: Literature review and research agenda. *The International Journal of Digital Accounting Research*, 21, 1–22. [\[CrossRef\]](#) [\[PubMed\]](#)
- Nyakarimi, S. (2022). Probable earning manipulation and fraud in banking sector. Empirical study from East Africa. *Cogent Economics & Finance*, 10(1), 2083477. [\[CrossRef\]](#)
- Ocampo, C. A. (2023). Detectando el fraude con inteligencia artificial: Una perspectiva avanzada en auditoría forense. *Revista La Junta*, 6(2), 13–40. [\[CrossRef\]](#)
- Onwubiko, C. (2020). Fraud matrix: A morphological and analysis-based classification and taxonomy of fraud. *Computers & Security*, 96, 101900. [\[CrossRef\]](#)
- Parlindungan, R., Africano, F., & Elizabeth, P. S. M. (2017). Financial statement fraud detection using published data based on fraud triangle theory. *Advanced Science Letters*, 23(8), 7054–7058. [\[CrossRef\]](#)
- Petra, S., & Spieler, A. C. (2020). Accounting scandals: Enron, worldcom, and global crossing. In *Corporate fraud exposed* (pp. 343–360). Emerald Publishing Limited. [\[CrossRef\]](#)
- Phong, N. A., Tam, P. H., & Tung, N. T. (2024). Identifying fraud financial reports based on signs of income management using machine learning technology: The case of listed companies in Vietnam. *Journal of International Commerce, Economics and Policy*, 15(2), 2450013. [\[CrossRef\]](#)
- Rahman, M. J., & Zhu, H. (2024). Detecting accounting fraud in family firms: Evidence from machine learning approaches. *Advances in Accounting*, 64, 100722. [\[CrossRef\]](#)
- Ramírez-Alpizar, A., Jenkins, M., Martínez, A., & Quesada-López, C. (2020). Use of data mining and machine learning techniques for fraud detection in financial statements: A systematic mapping study. *Revista Ibérica de Sistemas e Tecnologías de Informação*, E28, 97–109.
- Ramos, M., López, W., & Mateos, G. (2022). Importancia de las auditoria externas para el análisis efectivo de los estados financieros. *Revista de Investigación Académica Sin Frontera*, 37, 10. [\[CrossRef\]](#)

- Ranganatha, H. R., & Syed Mustafa, A. (2025). Enhancing fraud detection efficiency in mobile transactions through the integration of bidirectional 3d quasi-recurrent neural network and blockchain technologies. *Expert Systems with Applications*, 260, 125179. [\[CrossRef\]](#)
- Rao, R. K., & Mandhala, V. N. (2024). Unveiling financial fraud: A comprehensive review of machine learning and data mining techniques. *Ingénierie Des Systèmes d'Information*, 29(6), 2309–2334. [\[CrossRef\]](#)
- Rashid, M., Khan, N. U., Riaz, U., & Burton, B. (2023). Auditors' perspectives on financial fraud in Pakistan—Audacity and the need for legitimacy. *Journal of Accounting in Emerging Economies*, 13(1), 167–194. [\[CrossRef\]](#)
- Raudha, F., & Saeedi, M. (2019). Artificial intelligence and machine learning as a tool in preventing and detecting financial fraud: A systematic literature review. *Journal of Advanced Research in Dynamical and Control Systems*, 11(11), 904–911. [\[CrossRef\]](#)
- Reurink, A. (2018). Financial fraud: A literature review. *Journal of Economic Surveys*, 32(5), 1292–1325. [\[CrossRef\]](#)
- Rezaee, Z. (2005). Causes, consequences, and deterrence of financial statement fraud. *Critical Perspectives on Accounting*, 16(3), 277–298. [\[CrossRef\]](#)
- Robles Quiñónez, G. D., Egas Moreno, F. G., Benites Valverde, L. A., & Cifuentes Quiñónez, L. M. (2024). International accounting in Latin America: An overview of International Financial Reporting Standards (IFRS). *Sapienza: International Journal of Interdisciplinary Studies*, 5(2), e24040. [\[CrossRef\]](#)
- Rodríguez Salinas, J. (2023). Auditoría forense en la era de la inteligencia artificial, un enfoque vanguardista para combatir el fraude financiero. *Punto de Vista*, 14(21), 99–118. [\[CrossRef\]](#)
- Roszkowska, P. (2021). Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments. *Journal of Accounting & Organizational Change*, 17(2), 164–196. [\[CrossRef\]](#)
- Sarkar, S., & Spieler, A. C. (2020). Corporate fraud: The cases of Barings bank, Volkswagen, and HIH insurance. In *Corporate fraud exposed* (pp. 421–437). Emerald Publishing Limited. [\[CrossRef\]](#)
- Sawangarreerak, S., & Thanathamthee, P. (2021). Detecting and analyzing fraudulent patterns of financial statement for open innovation using discretization and association rule mining. *Journal of Open Innovation: Technology, Market, and Complexity*, 7(2), 128. [\[CrossRef\]](#)
- Scharff, M. M. (2005). Understanding WorldCom's accounting fraud: Did groupthink play a role? *Journal of Leadership & Organizational Studies*, 11(3), 109–118. [\[CrossRef\]](#)
- Sequeira, N., Mota, M., Costa, R., & Luty, P. (2024). The influence of the COVID-19 crisis on financial statements manipulations in the Portuguese wine and tourism sector. In *Advances in tourism, technology and systems. ICOTTS 2023* (pp. 483–493). Springer. [\[CrossRef\]](#)
- Setiawan, N., & Soewarno, N. (2025). The examination of asset misappropriations in managers' workplaces using hexagon's fraud and the moderating impact of perceived strength of internal control. *Journal of Financial Crime*, 32, 860–877. [\[CrossRef\]](#)
- Shahana, T., Lavanya, V., & Bhat, A. R. (2023). State of the art in financial statement fraud detection: A systematic review. *Technological Forecasting and Social Change*, 192, 122527. [\[CrossRef\]](#)
- Shi, W., Connelly, B. L., & Hoskisson, R. E. (2017). External corporate governance and financial fraud: Cognitive evaluation theory insights on agency theory prescriptions. *Strategic Management Journal*, 38(6), 1268–1286. [\[CrossRef\]](#)
- Souvenir, G., de Clerck, T., Schyvinck, C., Vermeersch, A., Hardyns, W., & Willem, A. (2025). From financial statement fraud to asset misappropriation: Fraud in nonprofit sports clubs and cultural underpinnings. *Deviant Behavior*, 1–17. [\[CrossRef\]](#)
- Srebro, B., Mavrenski, B., Bogojević Arsić, V., Knežević, S., Milašinović, M., & Travica, J. (2021). Bankruptcy risk prediction in ensuring the sustainable operation of agriculture companies. *Sustainability*, 13(14), 7712. [\[CrossRef\]](#)
- Suljić, M., Jusufović, A., Filipović, S., Suljić, E., & Gadžo, A. (2025). Data mining approach in detecting inaccurate financial statements in government-owned enterprises. *Croatian Operational Research Review*, 16(1), 1–15. [\[CrossRef\]](#)
- Tan, K.-L., Hii, I. S. H., Huang, Y., & Yan, Y. (2024). Reducing dishonest disclosures during expense reimbursement: Investigating the predictive power of the technology acceptance model with a corporate governance perspective. *Journal of Accounting & Organizational Change*, 20(5), 874–895. [\[CrossRef\]](#)
- Tawiah, V., & Gyapong, E. (2023). International financial reporting standards, domestic debt finance and institutional quality: Evidence from developing countries. *International Journal of Finance & Economics*, 28(3), 2915–2936. [\[CrossRef\]](#)
- Uygur, S. A., & Napier, C. J. (2024). Understanding fraud in the not-for-profit sector: A stakeholder perspective for charities. *Journal of Business Ethics*, 190(3), 569–588. [\[CrossRef\]](#)
- Van Driel, H. (2019). Financial fraud, scandals, and regulation: A conceptual framework and literature review. *Business History*, 61(8), 1259–1299. [\[CrossRef\]](#)
- Villaescusa, N., & Amat, O. (2022). When collusion meets the fraud triangle: A case study approach. *Journal of Financial Crime*, 29(3), 805–815. [\[CrossRef\]](#)
- Vizcarra, H. (2019). Influencing energy company climate disclosure practices: Cautionary words for state attorneys general. *SSRN Electronic Journal*, 1–5. [\[CrossRef\]](#)
- Wan, J. (2024). Bubble occurrence and landing. *Journal of Financial Stability*, 70, 101210. [\[CrossRef\]](#)

- Wan-Hussin, W. N., Fitri, H., & Salim, B. (2021). Audit committee chair overlap, chair expertise, and internal auditing practices: Evidence from Malaysia. *Journal of International Accounting, Auditing and Taxation*, 44, 100413. [\[CrossRef\]](#)
- West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security*, 57, 47–66. [\[CrossRef\]](#)
- Whiting, D. G., Hansen, J. V., McDonald, J. B., Albrecht, C., & Albrecht, W. S. (2012). Machine learning methods for detecting patterns of management fraud. *Computational Intelligence*, 28(4), 505–527. [\[CrossRef\]](#)
- Wu, H., Chang, Y., Li, J., & Zhu, X. (2022). Financial fraud risk analysis based on audit information knowledge graph. *Procedia Computer Science*, 199, 780–787. [\[CrossRef\]](#)
- Yang, L. (2022). An information quality-based explanation for loan loss allowance inadequacy during the 2008 financial crisis. *Journal of Accounting and Economics*, 73(1), 101433. [\[CrossRef\]](#)
- Yassine, H., Zahra, H., & Kezazy Hamza, E. (2024). Systematic review of IPSAS standards: The introduction of IPSAS in public establishments. *Edelweiss Applied Science and Technology*, 8(5), 292–306. [\[CrossRef\]](#)
- Zajmi, S. (2019). Principles of transparent financial reporting as the basis of financial statements quality control. *Poslovna Ekonomija*, 13(2), 60–68. [\[CrossRef\]](#)
- Zambrano Vargas, Y. (2017). La auditoría forense: Un mecanismo para detectar el fraude de estados financieros en Colombia. *Inquietud Empresarial*, 15(2), 13–36. [\[CrossRef\]](#)
- Zemankova, A. (2019, December 8–10). *Artificial intelligence in audit and accounting: Development, current trends, opportunities and threats—Literature review*. 2019 International Conference on Control, Artificial Intelligence, Robotics & Optimization (ICCAIRO), Athens, Greece. [\[CrossRef\]](#)
- Zhang, B., Zhang, Q., Huang, Z., Li, M., & Li, L. (2018). A multi-criteria detection scheme of collusive fraud organization for reputation aggregation in social networks. *Future Generation Computer Systems*, 79, 797–814. [\[CrossRef\]](#)
- Zhao, Y., Liu, R., Xue, J., Wu, Q., & Zhang, X. (2024). Environmental protection tax law and corporate financial fraud: Evidence from listed firms in China. *International Review of Financial Analysis*, 96, 103537. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.