Revista Catarinense da CIÊNCIA CONTÁBIL

ISSN 2237-7662, Florianópolis, SC, v. 24, 1-19, e3538, 2025

https://doi.org/10.16930/2237-7662202535382

Available at http://revista.crcsc.org.br

TRENDS AND APPLICATION OF DETERRENCE, DETECTION, AND PREVENTION TECHNIQUES IN COMBATING FINANCIAL FRAUD

LAURA PIANETTI DE BRUM[1]
Universidade Federal de Santa Catarina, Faculdade de Ciências Contábeis, Departamento de Ciências Contábeis, Florianópolis, SC, Brazil
https://orcid.org/0009-0000-2817-7922
laura.piannetti@gmail.com

LUIZA SANTANGELO REIS
Universidade Federal de Santa Catarina, Faculdade de Ciências Contábeis, Departamento de Ciências Contábeis, Florianópolis, SC, Brazil
https://orcid.org/0000-0002-0266-7410
luizasantangeloreis@gmail.com

ABSTRACT

This study aims to analyze the most researched techniques of deterrence, detection, and prevention of financial fraud between 2019 and 2024, through a systematic literature review using the ProKnow-C method. To this end, 45 articles retrieved from the Scopus, Google Scholar, and Web of Science databases and 12 reports from audit-related websites were selected to compose the bibliographic portfolio. Through a systemic analysis of the article portfolio, organized according to the three types of techniques, eight types of tools were identified and classified into three status categories. Among the findings, the detection technique emerged as the most researched, with Internal Control, Machine Learning, and Technologies/Software being the most frequently discussed tools. This highlights a more reactive than preventive approach in combating fraud. Based on the analysis of future trends presented in the audit-related reports, technology was identified as the most frequently cited and discussed theme among audit firms and anti-fraud associations, with various branches such as Machine Learning, biometrics, and databases. This research seeks to contribute by identifying the most researched techniques and tools, as well as those highlighted as future trends, while also comparing studies on traditional methods with innovative approaches and the use of emerging technologies, thereby broadening the discussion on the evolution of fraud prevention and detection.

Palavras-Chave: Anti-fraud. Techniques. Deterrence. Prevention. Detection.

Edited in Portuguese and English. Original version in Portuguese.

Version of the article presented at the 14th UFSC Congress on Controllership and Finance, held from June 26 to 28, 2024, in Florianópolis, SC, Brazil.

[1] **Correspondence address:** Rua Douglas Seabra Levier, 61 | Carvoeria | 80040-410 | Florianópolis, SC | Brazil.

Received on 09/25/2024. **Revised on** 03/20/2025. **Accepted on** 23/04/2025 by Prof. Dr. Rogério João Lunkes (Editor-in-Chief). **Published on** 05/30/2025.

1 INTRODUCTION

A study conducted by PwC Brazil (2022) gathered data from national and international companies that experienced some form of fraud. The study revealed that between 2020 and 2022 there was a 16% increase in the number of Brazilian companies that fell victim to fraud, while the number of international companies showed a 1% decrease. In terms of monetary values, the 2022 report by the Association of Certified Fraud Examiners (ACFE) indicated a total loss of $3.6 billion due to fraud. This amount was identified based on 2,110 fraud cases from 113 different countries.

Focusing on Latin America, a study conducted by Forrester in February 2024 reported that 60% of the organizations surveyed experienced an increase in fraud of 5% or more in the past year. Moreover, 83% of the executives interviewed stated that fraud further hinders the development of trust with customers.

Fraud is an illicit and dishonest act intentionally committed to obtain financial advantage for oneself or for third parties (Simanungkalit, Hertadi & ul Hosnah, 2024). In this regard, Simmons (1995) defines that fraud only occurs when three elements are present: an individual or organization intentionally acts in bad faith, a victim believes the information provided, and the victim relies on or acts based on the fraudulent information.

Corporate fraud and crimes are as old as organizations themselves, having existed even before the Industrial Revolution, and their impacts have had significant consequences for the global economy (Pearson & Singleton, 2008). Among the most common types of fraud are bribery, corruption, money laundering, forgery, and kickbacks. In this context, Pinheiro (2003) argues that fraud is one of the main obstacles to the growth and continuity of companies, highlighting that internal controls are outdated when compared to the continuous evolution of fraud schemes.

The sophistication of fraud strategies has become evident in the global landscape, which has been rapidly transforming in recent decades due to emerging technologies that evolve daily. This reality is no different in the financial and accounting sectors. According to Breda (2019), these changes are complex and may face resistance in their implementation. However, the improvements they can generate are evident, such as process optimization and error reduction. Over the years, scholars have highlighted the ongoing struggle to combat fraud, which continues to adapt to emerging vulnerabilities and, despite all efforts, remains a growing problem in terms of both frequency and severity. This new digital era has brought about significant changes in the practice of fraud, driven by a dynamic evolution and marked by increasingly sophisticated schemes that exploit technological advances (Daraojimba et al., 2023; Tatineni, 2020; Wolfe & Hermanson, 2004). This current scenario creates a need for stronger internal detection and prevention controls. An adequate and effective internal control system allows companies to create and preserve value and to reduce the risks to which they are constantly exposed (Cristovão, 2023; Silva et al., 2015; Henriques, 2022).

Thus, it becomes clear that fraud, in its various forms, is common across companies regardless of their size or sector (Henriques, 2022). It contributes to the weakening and bankruptcy of organizations, in addition to breaking consumer trust in brands and leading to mass layoffs. In order for companies to have the necessary structure and knowledge to combat fraud and, as a result, minimize its effects, it is essential to understand the different techniques and how they are currently applied.

In light of this context, the following research question was formulated: What are the most recent techniques for detecting and preventing financial fraud found in the literature? Based on this question, this article aims to analyze the use of deterrence, detection, and prevention techniques in financial fraud research conducted between 2019 and 2024.

As technology advances, so do the methods used to commit fraudulent acts. For this reason, the present study is justified by the need to understand what is currently being researched and

applied in the field of financial fraud prevention and which trends are emerging, so the market can be better prepared to face them. In practical terms, the study contributes to the improvement and reassessment of anti-fraud practices and techniques used in the daily operations of companies. In theoretical terms, it seeks to identify which practices should be further explored in the future, as well as to compare traditional methods with innovative approaches, such as the use of emerging technologies, thereby expanding the academic discussion on the evolution of anti-fraud strategies.

2 THEORETICAL FRAMEWORK

Fraud represents a significant threat to companies and organizations, accounting for billions in lost funds across both public and private sectors, and undermining integrity, efficiency, and financial stability worldwide (Solomon et al., 2023). Furthermore, fraud can lead to consequences such as reputational damage, loss of trust, financial hardship, project abandonment, organizational failure or liquidation, inefficient services or operations, and, in extreme cases, individual bankruptcy and economic distress (Samuel & Augustine, 2022; Tariq et al., 2024).

Traditional methodologies are increasingly proving insufficient to combat and detect fraudulent activities. This is because fraud is a complex mix of conditions and human motivations that continuously adapts (Koerniawan et al., 2022). Faced with the risk of fraud, the best measure companies can take is to find ways to prevent and avoid it (Fitrijanti et al., 2021), which can be achieved through the implementation of auditing techniques within organizations.

Auditing techniques can be divided into deterrence, prevention, and detection techniques. These techniques address the opportunity component of fraud, as their combined use creates an environment that can influence the potential fraudster's judgment regarding the likelihood of successfully committing and concealing the crime (Dorminey et al., 2012).

According to Paiva (2012), deterrence aims to persuade an individual not to act against the will of the party seeking to deter them, thus establishing limitations that lead to the abandonment of the initial intention. In this context, Wells (2004) argues that internal audits can help deter fraud, as their primary function is to monitor internal methods and their functioning (Rossi & Silva, 2016). External audits, in turn, can help discourage fraudulent managerial behavior and mitigate the risk of information asymmetry (Kassem, 2024).

Even when deterrence is not effective, prevention techniques play a major role in combating financial fraud (Santos et al., 2021). In a study conducted by Murphy and Dacin (2011), three psychological mechanisms leading to fraudulent behavior are identified: (1) lack of awareness, (2) intuition combined with rationalization, and (3) reasoning. The authors emphasize that organizations should design preventive methods that counteract these mechanisms. Establishing a culture of integrity, ethics, and accountability is essential for fraud prevention and can be achieved by promoting ethical behavior, setting clear expectations, and fostering a transparent environment (Solomon et al., 2023).

However, when deterrence and prevention efforts are not sufficient, the organization must have a structured process to detect fraud. Dorminey et al. (2012) note that a key aspect of fraud detection is to design an audit plan focused on helping auditors identify vulnerabilities within the system. In this regard, Santos et al. (2023) add that auditing is fundamental for detecting fraud, as it relies on regulations and standards to analyze financial statements, thereby reducing risks that could lead to financial losses within organizations.

According to a study by PwC (2022), recent years have seen an increase in threats posed by organized external actors who infiltrate the digital platforms of organizations. To be prepared to respond to these risks, companies and auditors must be more agile, developing and applying new approaches and tools for deterrence, prevention, and detection (Kassem, 2024). As new

techniques and technologies are created to mitigate fraud, new methods of committing fraudulent acts also emerge in parallel, making the continuous updating of these techniques essential.

Auditors and companies must understand the importance of new technologies and the skills required to use them appropriately, thereby delivering a more modern, digital, and intelligent audit that is capable of addressing both internal and external threats to which organizations are exposed (Eke et al., 2023). These efforts aim to protect the organization's assets, reputation, and financial well-being by implementing measures, tactics, methods, and best practices to identify and mitigate fraud risks before they result in harm (Solomon et al., 2023; Tariq et al., 2024).

For auditing techniques to be effective, change must extend beyond investment in new technologies and include transformations in how businesses operate (Eke et al., 2023). To be fortified and prepared to defend against fraud, companies must be familiar with current deterrence, prevention, and detection techniques, as well as with future trends in anti-fraud efforts.

Some research has already moved in this direction. For instance, the study by Mangala and Kumari (2015) reviewed research from 1984 to 2014 on the motivations behind fraud and strategies for combating it, highlighting warning signs and providing an overview of fraud detection and prevention techniques. Prenzler (2019), in turn, used case studies to identify interventions capable of preventing fraud. However, the present study is broader in scope and seeks to provide a forward-looking perspective on how to deter, prevent, or detect fraud within organizations.

3 METHODOLOGICAL PROCEDURES

The instrument selected to conduct the systematic literature review was the Knowledge Development Process – Constructivist (ProKnow-C). ProKnow-C originated at the Federal University of Santa Catarina, within the Laboratory of Multicriteria Methodology for Decision Aiding (LabMCDA), and consists of a process used to research, analyze, and select scientific articles and other literature through a structured four-step method: (i) selection of a portfolio of relevant articles; (ii) bibliometric analysis of the portfolio; (iii) systemic analysis; and (iv) definition of the research problem and objective (Ensslin et al., 2010; Ensslin et al., 2013).

The ProKnow-C method allows researchers to structure a bibliographic portfolio within their area of interest, taking into account the limitations and constraints of the research. These boundaries, defined by the researcher, are influenced by the context in which they are situated and by their access to the available published studies (Ensslin et al., 2013; Linhares et al., 2019).

In the portfolio selection phase, scientific databases were used to collect peer-reviewed articles in order to identify which techniques and tools are being researched, while reports were collected from auditing websites to identify current market discussions. Based on the search conducted between February 22 and March 7, 2024, across three academic databases and six auditing websites (presented in Table 1), a total of 57,603 articles and 2,158 reports related to the research topic were found.

Table 1

Databases and Filters Used for Portfolio Composition

Databases Searched: (i) Scopus, (ii) Google Scholar, (iii) Web of Science	**Websites Searched:** (i) EY (ii) PwC (iii) KPMG (iv) AFC (v) ACFE (vi) Banco Central
Search Fields: (i) Title, (ii) Abstract , (iii) Keywords	**Search Fields:** (i) Título
Keywords: (i) Audit ,(ii) Prevention , (iii) Detection	**Keywords:** (i) Audit (ii) Prevention (iii) Detection (iv) Deterrence

(iv) Deterrence	
Search Command: (i) "audit" and "prevention" or "detection" or "deterrence"	**Search Command:** (i) “fraud” OR "audit" OR "prevention" OR "detection" OR "deterrence"
Publication Date 2019 - 2024	**Publication Date** 2019 - 2024

Source: Prepared by the authors.

After compiling the literature portfolio, the second stage of the ProKnow-C method was carried out: the bibliometric analysis, which was applied exclusively to the scientific articles. Bibliometric analysis is a methodology based on counting bibliographic content, grounded in the quantification of parameters within a set of articles, with the aim of managing information and scientific knowledge related to a specific topic (Silva et al., 2011; Lacerda et al., 2012). The following parameters were analyzed: year of publication, deterrence, prevention, and detection techniques, future trends in auditing techniques, and practical outcomes achieved.

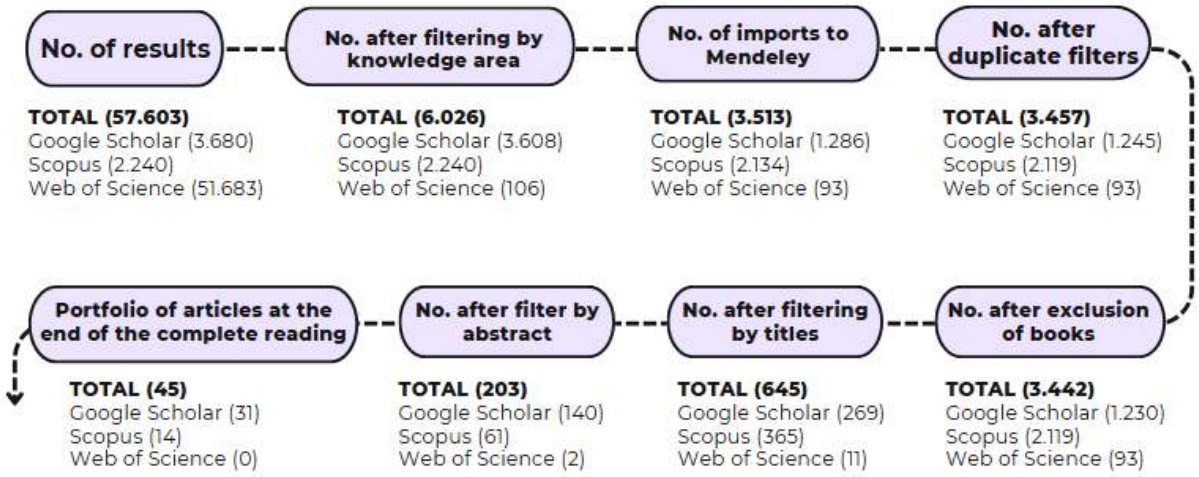
Based on these parameters, the following questions will be addressed:(i) What deterrence, prevention, and detection techniques are cited in the research?(ii) How are the tools applied within the different techniques? (iii) What are the implications analyzed in the studies??

For the bibliometric analysis, the software Mendeley was used—a reference management tool developed by Elsevier to manage and share research documents and assist in optimizing the organization and access of reference files (Farias et al., 2019).

Before importing the articles from the Web of Science database into Mendeley, a filtering by field of knowledge was performed due to the large volume of results, reducing the number of articles from 51,863 to 106. During the import process from Google Scholar and Scopus into the software, some articles failed to import successfully, resulting in a reduction of 2,500 articles (Figure 1).

Figure 1

Bibliometric analysis of articles



Source: Prepared by the authors.

After reducing the number of articles imported from the databases, Mendeley totaled 3,513 articles for bibliographic analysis. With the help of the software, 56 duplicate articles and 15 books

were identified. After removing these references, the database consisted of 3,442 articles. The titles of these 3,442 articles were then reviewed to assess their alignment with the research topic. At this stage, 2,797 articles were excluded. Among the remaining 645 articles, the abstracts were read, and 442 were found to be unrelated to the research theme. After this filtering based on abstract evaluation, a total of 203 articles remained. These 203 articles were read in full, and 45 articles were selected to compose the study for meeting the established criteria.

The bibliometric analysis of the reports found on auditing websites was conducted through a review of their titles and the content discussed. After excluding the reports that were not aligned with the research topic, 12 reports were selected to be included in the portfolio.

The analysis of the 45 articles that make up the bibliographic portfolio was segmented according to the three types of fraud-combat techniques. These three techniques are applied at different stages of fraud development: deterrence and prevention techniques are applied before the fraud occurs, while detection techniques are applied after the fraud has taken place. This division provides a clearer understanding of how the researched tools were applied, contributing to the comprehension of the different uses of the same tool at various stages of the fraud.

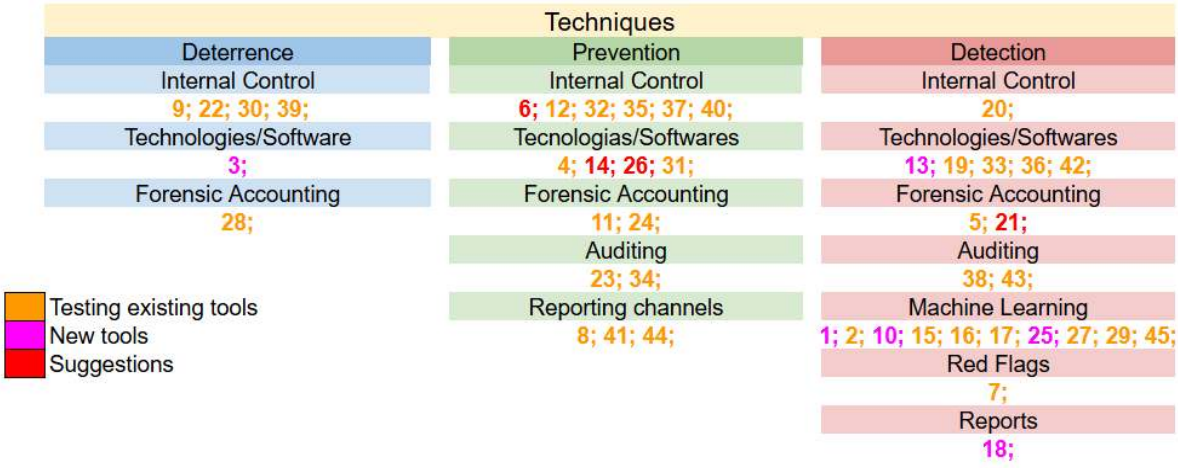
4 RESEARCH RESULTS

4.1 Systemic Analysis of the Portfolio

The systemic analysis corresponds to the third stage of the ProKnow-C methodology, in which the 45 selected articles were categorized according to three types of fraud-combat techniques: deterrence, prevention, and detection. Within this systemic analysis, eight types of techniques and three statuses of the tools discussed were identified (testing of existing tools, new tools, and suggestions). These classifications serve as the foundation for the research analysis (Figure 2).

Figure 2

Systemic Analysis of the Articles by Technique, Type, and Status



Source: Prepared by the authors.

According to the Institute of Internal Auditors of Brazil (IIA) (2008), the governance of an entity and its management core components of internal control aim to ensure that the entity achieves its objectives. To this end, they are composed of processes that inform, direct, manage, and monitor organizational activities. The use of internal control within organizations may serve preventive, detective, or corrective purposes (Lima et al., 2012).

According to Figure 2, internal control is present in all three techniques: deterrence, prevention, and detection, aligning with the assertion by Lima et al. (2012). However, research and practical applications are more frequent in deterrence and prevention techniques (36% and 54%, respectively). In most studies from the bibliographic portfolio, internal control tools are composed of sets of actions that, together, become effective in combating fraud. Among the most cited are the Fraud Control Plan (FCP) (Koerniawan et al., 2022; Wicaksono & Yuhertiana, 2020), risk assessments or committees (Abdullah et al., 2019; Dagane, 2024; Nuswantara, 2020), and corporate and governmental governance (Fitrijanti et al., 2021; Ubesie et al., 2023).

The same trend can be observed with Technologies/Software and Forensic Accounting: while both are researched across all three techniques, their emphasis is greater in prevention (40% each) and detection (50% and 40%, respectively).

Technologies/Software encompass information technologies and data analytics that enable the expansion of new fraud detection methods, often operating in collaboration with auditors and other experts (Singh et al., 2019). This collaboration can save time and resources, allowing auditors to spend less time designing and implementing methods for structured and unstructured data and more time analyzing critical information (Rosnidah et al., 2022).

Among the Technologies/Software identified in the bibliographic portfolio, Artificial Intelligence (AI) and Computer-Assisted Audit Techniques (CAATs) appear in multiple studies (Eke et al., 2023; Mohammed & Rahman, 2024; Rosnidah et al., 2022; Roszkowska, 2021). Other cited technologies include Blockchain, Big Data, and Multilayer Neural Networks, which are already well-known and widely used (Rosnidah et al., 2022; Roszkowska, 2021; Ruzgas et al., 2023). Additionally, newer tools such as alert-generating algorithms and predictive analytics models are being applied (Ahmed et al., 2021; Singh et al., 2019).

Many of the technologies and software currently in use are part of Forensic Accounting techniques, as this field incorporates a contemporary approach that significantly contributes to the investigation and handling of financial information (Özcan, 2019). The rise in fraud has driven companies to invest in and specialize in Forensic Accounting to uncover irregularities and prevent their occurrence. This area of accounting has emerged as a dynamic tool and strategic approach in the fight against corruption, crime, and fraud (Abdullahi et al., 2023).

This specialization is evident in the portfolio, which presents results from the use of Forensic Accounting in various areas and activities, such as financial indicator analysis (Özcan, 2019), data mining (Akinleye et al., 2023), and support for police, lawyers, courts, regulatory bodies, crime-fighting agencies, and other institutions in the investigation, detection, and documentation of fraud (Richmond & Okoye, 2019).

Auditing is widely cited when it comes to prevention and detection techniques. It involves a review process of organizational activities to ensure compliance with established regulations, identify corrections, and verify the legality of records based on accounting principles (Silva, 2022). However, due to the increasing complexity of fraud, the role of auditing is expanding, and the market is demanding that it take a more active role in directly combating fraud. Therefore, it is crucial that auditors understand the changes needed to meet these expectations (Abdullah et al., 2023; Samuel & Augustine, 2022).

According to Figure 2, research related to auditing is equally divided between prevention and detection techniques (50% each). However, when analyzing the tools addressed, 75% of the studies refer to internal audits and 25% to external audits. The portfolio results indicate a concern with the effectiveness and improvement of internal tools within organizations. This aligns with findings from an external audit study by Kassem (2024), which states that the motivations and integrity of senior management are among the most critical factors in fraud risk assessment. However, because external auditors are not embedded within the organization, they often lack

sufficient information to assess these factors unlike internal auditors, who have broader access and a more complete view of the risk landscape (Kassem, 2024).

Studies show that internal auditing has a significant influence on fraud prevention, and it can combat fraud at various stages. They also conclude that an efficient, competent, and cooperative audit team can detect financial and administrative fraud (Ibrahim & Al-Haidari, 2022; Samuel et al., 2022). Among the technical methods that support auditors in preventing and detecting fraud are Embedded Audit Modules, the Monitoring and Control Layer, Audit Data Warehousing, and the Audit Applications Approach (Abdullah et al., 2023).

Within audit techniques particularly internal audit Whistleblowing Channels are among the most widely used tools by organizations. They provide a mechanism for reporting workplace violations or unethical behavior by internal or external actors (Handajani et al., 2022). These channels encourage employee and community participation, fostering a willingness to act and helping to reduce the culture of silence, thereby contributing directly and indirectly to fraud prevention (Maulida & Bayunitri, 2021).

In the bibliographic portfolio, this tool appears exclusively in prevention techniques, although it is also used in fraud and crime detection. This is because research indicates that enhancing whistleblowing channels can and should serve as a preventive measure to identify suspicious behaviors before fraud materializes (Achyarsyah, 2022; Awotomilusi & Ogunleye, 2021; Maulida et al., 2021).

Among the three techniques identified in this article deterrence, prevention, and detection detection has the largest number of studies and consequently the greatest number of tools discussed. This is the case with Machine Learning, Red Flags, and Reports, which are used exclusively for detecting fraud.

Machine Learning is a subset of AI involving algorithms and statistical models that allow computers to learn from and analyze large volumes of data. This tool significantly reduces reliance on traditional labor and enhances the efficiency of detecting patterns and anomalies in financial information (Chen & Yan, 2022; Matar, 2023).

Approximately 40% of the portfolio consists of detection models based on Machine Learning, developed and tested through various approaches. These include the ID3 decision tree (Kootanaee et al., 2021), the stacking algorithm (Chen & Wu, 2022), the Recurrent Neural Network (RNN) and Long Short-Term Memory (LSTM) (Jan, 2021), and the XGBoost and GAN models (Lu et al., 2023). Some models achieved up to 94% accuracy in fraud detection.

Machine learning algorithms are also widely explored in the research, accounting for 40% of the portfolio. These studies aim to optimize and expand the use of such algorithms in areas such as the detection of anomalous daily journal entries (Bakumenko & Elragal, 2022), support for forensic accountants in criminal accounting (Matar, 2023), selection of high-risk taxpayers for auditing (Lee, 2022), and implementation of full-population audit approaches (Chen et al., 2022).

Red Flags are mentioned exclusively within the detection technique (Figure 2), but they are valuable in various stages of fraud, as they represent events, pressures, opportunities, or personal characteristics that may trigger fraudulent intent. As such, they can be used as early warning mechanisms (Magro & Cunha, 2017).

Hijazi and Mahboub (2019) base their study on International Standard on Auditing (ISA) 240 to determine whether Red Flags are related to the detection of Fraudulent Financial Reporting (FFR). Their findings indicate a positive influence of Red Flag use by accountants in identifying fraud. However, out of the 41 Red Flags recommended by ISA 240, only 7 had a strong presence in the company analyzed. This suggests that Red Flags must be adapted to the specific context and organization where they are applied as a detection tool.

Company reports can be interpreted as representations of an entity's economic reality, shaped by the interpretations of executives, managers, and other stakeholders involved in their

preparation (Ribeiro, 2014). Therefore, they are an important component in audit evaluations of potential fraud.

According to Zhang et al. (2022), one report worth analyzing is the Management Discussion and Analysis (MD&A), an annual and quarterly report published by publicly traded companies in China. Their study used various vector indices, the Bag of Words (BoW) model, and machine learning algorithms to analyze these reports. The results demonstrated predictive effectiveness and fraud recognition capability, with the BoW model correctly identifying 77% of fraudulent reports. According to the authors, this tool may be useful for audit authorities in identifying fraudulent reporting.

4.1.1 Development Stage of the Tools

Through the systemic analysis of the bibliographic portfolio, it was possible to classify the tools into three different statuses: testing of existing tools, new tools, and suggestions. This classification can be used to understand the approach taken by researchers in recent years regarding deterrence, prevention, and detection tools.

Testing of existing tools accounts for more than 77% of the bibliographic portfolio and is present across all three techniques: deterrence, prevention, and detection. This indicates that, in recent years, researchers have focused on applying already established tools while exploring their effectiveness and efficiency in different business contexts and processes. Examples of such tests of existing tools can be found in studies addressing Auditing (Abdullah et al., 2023; Ibrahim et al., 2022; Samuel & Augustine, 2022), Whistleblowing Channels (Achyarsyah, 2022; Awotomilusi et al., 2021; Maulida et al., 2021), Internal Control (Dagane, 2024; Fitrijanti et al., 2021), Red Flags (Hijazi et al., 2019), Technologies/Software (Ruzgas et al., 2023; Samagaio & Diogo, 2022), Forensic Accounting (Abdullahi et al., 2023), and Machine Learning (Achyarsyah, 2022; Kootanaee et al., 2021).

The “new tool” status was assigned to studies that developed new tools or used existing foundations with a new approach. This status was identified in both deterrence and detection techniques, representing approximately 13% of the bibliographic portfolio. Tools with this status include Technologies/Software (Ahmed et al., 2021; Singh et al., 2019), Machine Learning (Chen et al., 2022; Lu et al., 2023), and Reports (Zhang et al., 2022).

Tools that did not fit into the categories of tested existing tools or new tools were classified as suggestions. These studies did not apply the tools in specific or practical cases but explored the theoretical basis to argue for their relevance and potential application. This status appeared only within prevention and detection techniques and accounted for approximately 8% of the bibliographic portfolio. Among the authors presenting tool suggestions are Rosnidah et al. (2022) and Roszkowska (2021) within Technologies/Software, Solomon et al. (2023) for Internal Control, and Richmond et al. (2019) for Forensic Accounting.

4.1.2 Basic Bibliometric Analysis

The articles that make up the bibliographic portfolio were analyzed by classification, and based on this analysis, a table was created to highlight the percentage of each technique and tool represented within the portfolio.

Figure 3
Percentage analysis of articles by technique and tool

Types of techniques					
	Deterrence	Prevention	Detection	Total	Percental
Internal Control	4	6	1	11	**24,44%**
Technologies/Softwares	1	4	5	10	**22,22%**
Forence Accounting	1	2	2	5	**11,11%**
Auditing	-	2	2	4	**8,89%**
Reporting channels	-	3	-	3	**6,67%**
Machine Learning	-	-	10	10	**22,22%**
Red Flags	-	-	1	1	**2,22%**
Reports	-	-	1	1	**2,22%**
Total	**6**	**17**	**22**	**45**	**100,00%**
Percentage	**13,33%**	**37,78%**	**48,89%**	**100,00%**	

Source: Prepared by the authors.

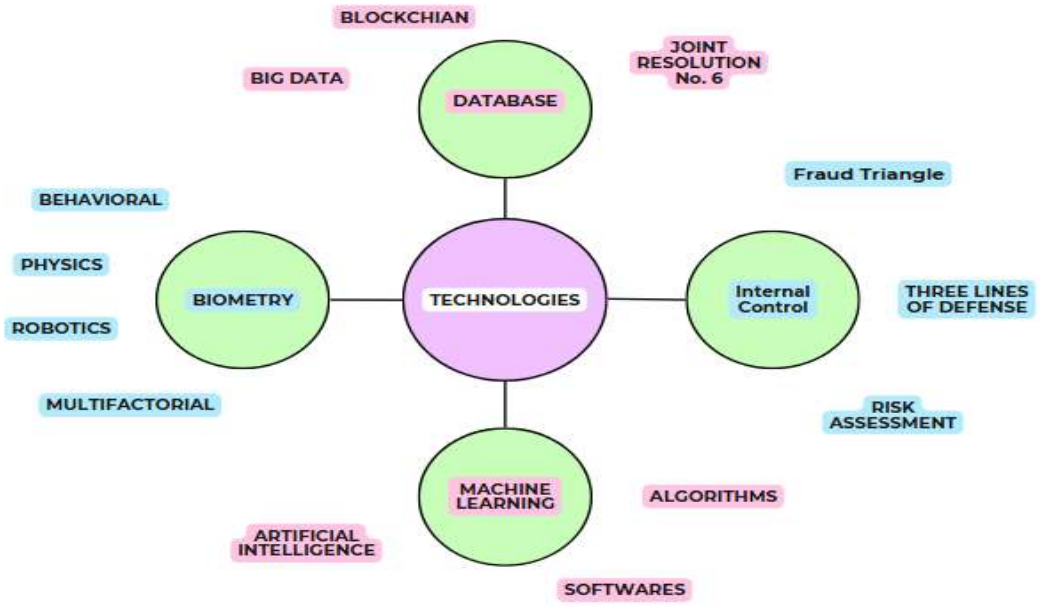
It was observed that the detection technique was the most researched in recent years, accounting for nearly 49% of the portfolio. In terms of tools, Internal Control was the most frequently cited, representing nearly 25% of the portfolio, followed by Technology/Software and Machine Learning tools, each with just over 22% representation.

4.2 Trends in Auditing Techniques

Another objective of this research is to analyze the future trends proposed by the articles and audit-related reports. Of the 45 articles included in the bibliographic portfolio, 22 contain recommendations and suggestions for future research, while the 12 audit website reports offer proposals to enhance deterrence, prevention, and detection techniques.

Among the 34 sources (articles and audit reports) that presented future suggestions, 19 are related to technologies, including Machine Learning, artificial intelligence, biometrics, learning algorithms, software, and databases. Another prominent tool was internal control, encompassing elements such as annual fraud training and collaboration with boards of directors, audit committees, standard setters, regulators, and other stakeholders.

Figure 4
Future Trends Map



Source: Prepared by the authors.

It is evident that technology is the most researched and recommended tool, both in the articles and in the reports from audit-related websites. Technology is a broad tool with a wide range of applications. Within the bibliographic portfolio, four main subdivisions emerged in which it played a significant role: Machine Learning, databases, biometrics, and internal control.

Machine Learning appears in both practical research, involving algorithms, software, and Artificial Intelligence (AI), and in audit-related reports. One such report by the Association of Certified Fraud Examiners (ACFE) surveyed market usage and found that 83% of the companies interviewed intend to implement AI into their anti-fraud programs within the next two years. The report also projects that the use of AI and Machine Learning in such programs is expected to triple over the same period (ACFE, 2024).

The audit firm Ernst & Young (EY) has highlighted biometrics as an emerging technology, particularly in the verification and authentication of identities. According to the report, biometric data can include fingerprints, signatures, or voice patterns and is categorized into physical, robotic, behavioral, and multifactor types (Figure 3). Regarding the use of biometrics and robotics, there was an increase in adoption between 2019 and 2024 of 14% and 11%, respectively (ACFE, 2024).

In its reports, EY also emphasizes the importance of data mining, analysis, and interpretation. However, it notes that the main challenge lies in acquiring a relevant database, as variables such as system infrastructure, formatting issues, or data privacy regulations may hinder this process. According to research conducted by ACFE, 9 out of 10 companies already use data analysis as part of their anti-fraud programs. Another noteworthy contribution to database usage is Brazil's Joint Resolution No. 6, dated May 23, 2023, issued by the Central Bank (BC), which addresses the creation of a centralized database containing information on suspected fraud indicators, to be shared electronically. The objective of this centralized database is to reduce the occurrence of fraud within the National Financial System, with implementation scheduled by November 1, 2023.

In the area of internal control, the recommendations focus on corporate culture and behavioral factors to support fraud detection. With advances in technology and research on human

behavior, it is now possible to improve the evaluation of pressure and rationalization elements, and, as a result, enhance the fraud risk assessment process (Ernst & Young, 2020).

Some gaps in the study were also identified that could be addressed in future research. One such gap is the lack of comparative analyses between technologies. Since technology is the most frequently addressed technique, comparing traditional methods with emerging ones would be particularly relevant. Another gap that could be explored is the cost-benefit analysis of implementing these techniques within companies, taking into account variables such as industry sector and organizational size.

5 FINAL CONSIDERATIONS

The objective of this study was to analyze the use of deterrence, prevention, and detection techniques for financial fraud as researched in the literature between 2019 and 2024, through a bibliographic review. It also aimed to identify future trends related to these techniques by analyzing reports from auditing websites that reflect current market discussions on combating financial fraud.

We conclude that detection techniques are the most researched, with approximately 49% of the articles in the portfolio addressing this approach, revealing a more reactive than preventive stance in fraud mitigation. Regarding the types of techniques identified in the analysis, Internal Control, Machine Learning, and Technologies/Software were the most frequently addressed tools. Internal Control and Technologies/Software were applied across deterrence, prevention, and detection techniques, whereas Machine Learning was used exclusively in detection techniques.

Through the analysis of future trends, it became evident that technology is the most cited and discussed theme among audit firms and associations engaged in combating fraud. The technological avenues identified include Machine Learning, biometrics, and databases. Some studies demonstrated the application of these technologies already in practice, while others highlighted their potential usefulness. From a broader perspective based on the analyzed portfolio, we found that technology is the most recurrent and widely applied theme in the context of combating financial fraud. This trend aligns with the increasingly sophisticated methods used to perpetrate fraud, indicating that the market and relevant associations recognize the importance of this tool.

This study has limitations, such as the data sources, which consisted solely of open-access articles and reports from audit-related websites, thereby excluding research requiring paid access. Among the suggestions for future research is the investigation of how these techniques are applied across different market sectors. Another potential direction is to examine the barriers and facilitators involved in the practical implementation of these techniques in audit processes. Ultimately, this study aimed to contribute on a practical level, by supporting the improvement of anti-fraud practices and techniques used in everyday business operations, and on a theoretical level, by identifying which practices should be further explored in future research to keep pace with the evolution of fraud schemes.

REFERENCES

Abdullah, A. M., Mousa, A. A., Abdulrahman, A. M., Mesfer, A. N., Mohammed, A. A., Salman, A. K., ... & Nasser, A. M. (2023). The Role of Modern Technology in Preventing and Detecting Accounting Fraud. *International Journal of Multidisciplinary Innovation and Research Methodology*, *2*(2), 1–10. https://ijmirm.com/index.php/ijmirm/article/view/13

Abdullahi, F. A., Mamuda, A. U., & Kauji, M. B. (2023). Feasibility of Implementing Forensic Accounting in Fraud Detection and Prevention in Public Sector: Evidence from Borno State. *International Journal of Social Sciences and Humanities*, *11*(6), 118–128. https://doi.org/2726577411167

Abdullah, W. N., Said, R., & Caliyurt, K. (2019). The Effect of Internal Governance on Corporate Financial Crime of Companies in Malaysia. *Journal of Governance and Integrity, 2*(2), 53–64. https://doi.org/10.15282/jgi.2.2.2019.5468

Ahmed, M., Ansar, K., Muckley, C. B., Khan, A., Anjum, A., & Talha, M. (2021). A semantic rule based digital fraud detection. *PeerJ Computer Science, 7,* e649. https://doi.org/10.7717/peerj-cs.649

Achyarsyah, P. (2022). Can investigative audit and whistleblowing systems prevent fraud?. *Atestasi: Jurnal Ilmiah Akuntansi, 5*(1), 124–136. https://doi.org/10.57178/atestasi.v5i1.31

Akinleye, G. T., Olatunji, O. F., Bolaji, Y. A., & Dauda, A. A. (2023). Combating Financial Crimes through Forensic Audit: Evidence from Nigeria. B*rit J Manag Mark Stud, 6*(4), 54–62. https://doi.org/10.52589/BJMMS-SRPHNYLN

Associação de Examinadores Certificados de Fraudes. (2024). *Anti-Fraud Technology Benchmarking Report 2024*. https://www.acfe.com/-/media/files/acfe/pdfs/sas_benchmarkingreport_2024.pdf

Associação de Examinadores Certificados de Fraudes. (2022). Occupational Fraud 2022: A Report to the nations. https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf.

Awotomilusi, N. S., & Ogunleye, A. W. (2021). Whistleblowing Policy and Fraud Prevention and Detection of Listed Deposit Money Banks: Experience from Ekiti State, Nigeria. *International Journal of Accounting, Finance and Risk Management*, *6*(4), 112–120. https://doi.org/10.11648/j.ijafrm.20210604.13

Banco Central do Brasil. (2023). *Resolução Conjunta n° 6 de 23/5/2023*. https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20Conjunta&numero=6

Bakumenko, A., & Elragal, A. (2022). Detecting anomalies in financial data using machine learning algorithms. *Systems, 10*(5), 130. https://doi.org/10.3390/systems10050130

Breda, Z. I. (2019). Uma reflexão sobre os impactos da tecnologia na Contabilidade. *Conselho Federal de Contabilidade, 8*.https://cfc.org.br/destaque/uma-reflexao-sobre-os-impactos-da-tecnologia-na-contabilidade/

Chen, Y., & Wu, Z. (2022). Financial fraud detection of listed companies in china: A machine learning approach. *Sustainability, 15*(1), 105. https://doi.org/10.3390/su15010105

Chen, Y., Wu, Z., & Yan, H. (2022). A full population auditing method based on machine learning. *Sustainability, 14*(24), 17008. https://doi.org/10.3390/su142417008

Cristovão, R. B. (2023). *Detecção de fraudes em cartão de crédito: um caso de uso de modelos supervisionados no e-commerce brasileiro*. [Doctoral dissertation, Universidade de São Paulo]. Digital Library USP. https://www.teses.usp.br/teses/disponiveis/55/55137/tde-23082023-102023/en.php.

Dagane, M. D. (2024). Effect of Internal Controls on Fraud Detection of Manufacturing Firms in Garissa County, Kenya. *International Journal of Finance*, *9*(1), 20–42. https://ideas.repec.org/a/bhx/ojtijf/v9y2024i1p20-42id1632.html

Daraojimba, R. E., Farayola, O. A., Olatoye, F. O., Mhlongo, N., & Oke, T. T. (2023). Forensic accounting in the digital age: a US perspective: scrutinizing methods and challenges in digital financial fraud prevention. *Finance & Accounting Research Journal, 5*(11), 342–360. https://doi.org/10.51594/farj.v5i11.614

Dorminey, J., Fleming, A. S., Kranacher, M. J., & Riley Jr, R. A. (2012). The evolution of fraud theory. *Issues in accounting education, 27*(2), 555–579. https://doi.org/10.2308/iace-50131

Eke, F., Egbodor, E., & Obayagbonna, E. O. (2023). An Appraisal of Computerized Auditing and Fraud Control In Edo State Nigeria. *Advance Journal of Financial Innovation and Reporting*, *7*(8), 1–20. https://www.wr-publishing.org/wp-content/uploads/IJARBM-Ezeonwuka-Le-Roux-Ogbodo-Generalized-Audti-Software-Internal-Auditing.pdf

Ensslin, L., Ensslin, S. R., Lacerda, R. T. O., & Tasca, J. E. (2010). ProKnow-C: Processo de análise sistêmica. Brasil: Processo técnico com patente de registro pendente junto ao INPI, 71–91.

Ensslin, L., Ensslin, S. R., & Pinto, H. D. M. (2013). Processo de investigação e Análise bibliométrica: Avaliação da Qualidade dos Serviços Bancários. *Revista de administração contemporânea, 17*, 325–349. https://doi.org/10.1590/S1415-65552013000300005

Ernst & Young. (2020). Preventing and detecting fraud: Strengthening the roles of companies, auditors and regulators. https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/ey-preventing-and-detecting-fraud.pdf

Farias, I. M. S., da Silva, R. R., & Silva, S. P. (2019). Gerenciador de referências Mendeley: características e uso no contexto de um grupo de estudos de Pós-Graduação em Educação. *Plurais-Revista Multidisciplinar, 4*(2), 65–79. https://doi.org/10.29378/plurais.2447-9373.2019.v4.n2.65-79

Fitrijanti, T., Soemantri, Ak, S. E. M. S., & Sofia, CA, S. (2021). Influence of Whistleblowing Systems, Effectiveness of Intenal Audits and Good Government Governance on Fraud Prevention. *International Journal of Innovative Science and Research Technology, 6*(11), 2456–2165. https://ijisrt.com/assets/upload/files/IJISRT21NOV031.pdf

Forrester Consulting. (2024). *Estudo do real custo de fraude na América Latina*. True-Cost-of-Fraud-2023-LATAM-Portuguese[1].pdf

Handajani, L., Muhsyaf, S., & Sokarina, A. (2022). The Effectiveness of Corporate Governance and Whistleblowing System on Fraud Disclosure. *Jurnal Ilmiah Akuntansi dan Bisnis*, *18*(1), 29–42. https://doi.org/10.24843/JIAB.2023.v18.i01.p03

Henriques, G. F. L. (2022). O contributo da auditoria para a prevenção e deteção de fraude. Uma aplicação ao setor bancário. [Doctoral dissertation, Instituto Superior de Contabilidade e Administração de Lisboa]. *Repositório Científico ISCAL.* http://hdl.handle.net/10400.21/15433

Hijazi, W., & Mahboub, R. M. (2019). Auditors perceptions towards the effectiveness of the international standard on auditing 240 Red Flags: Evidence from Lebanon. *International Journal of Economics & Business Administration, 7*(1), 162–173. https://www.um.edu.mt/library/oar/handle/123456789/43965

Ibrahim, M. A., & Al-Haidari, W. H. S. (2022). The effectiveness of internal audit process and team in detecting the financial and administrative corruption in the Iraqi public sector. *International Journal of Economics and Finance Studies*, *14*(03), 211–226. https://www.researchgate.net/publication/366952947_The_Effectiveness_of_Internal_Audit_Process_and_Team_in_Detecting_the_Financial_and_Administrative_Corruption_in_the_Iraqi_Public_Sector

The Institute of Internal Auditor. (2008). *Normas Internacionais para a Prática Profissional de Auditoria Interna*. https://iiabrasil.org.br/korbilload/upl/ippf/downloads/normasinternaci-ippf-00000001-02042018191815.pdf

Jan, C. L. (2021). Detection of financial statement fraud using deep learning for sustainable development of capital markets under information asymmetry. *Sustainability, 13*(17), 9879. https://doi.org/10.3390/su13179879

Kootanaee, A. J., Aghajan, A. A. P., & Shirvani, M. H. (2021). A hybrid model based on machine learning and genetic algorithm for detecting fraud in financial statements. *Journal of Optimization in Industrial Engineering, 14*(2), 169–186. https://doi.org/10.22094/JOIE.2020.1877455.1685

Kassem, R. (2024). External auditors' use and perceptions of fraud factors in assessing fraudulent financial reporting risk (FFRR): Implications for audit policy and practice. *Security Journal, 37*(3), 875-902. https://doi.org/10.1057/s41284-023-00399-w

Koerniawan, K. A., Afiah, N. N., Sueb, M., & Suprijadi, J. (2022). Fraud Deterrence: The Management's Intention In Using FCP. *Quality-Access to Succes, 23*, 190. https://doi.org/10.47750/QAS/23.190.31

Kootanaee, A. J., Aghajan, A. A. P., & Shirvani, M. H. (2021). A hybrid model based on machine learning and genetic algorithm for detecting fraud in financial statements. *Journal of Optimization in Industrial Engineering, 14*(2), 169–186. https://doi.org/10.22094/JOIE.2020.1877455.1685

Lacerda, R. T. D. O., Ensslin, L., & Ensslin, S. R. (2012). Uma análise bibliométrica da literatura sobre estratégia e avaliação de desempenho. *Gestão & Produção, 19*, 59–78. https://doi.org/10.1590/S0104-530X2012000100005

Lee, C. (2022). Deep learning-based detection of tax frauds: an application to property acquisition tax. *Data Technologies and Applications, 56*(3), 329–341. https://doi.org/10.1108/DTA-06-2021-0134

Lima, H. M. A., Melo, F. A. D. O., Reis, P. N. C., Lima, C. C. D. S., & Oliveira, V. M. D. S. (2012). Controle interno como ferramenta essencial contra erros e fraudes dentro das organizações. *Simpósio de Excelência em Gestão e Tecnologia-SEGeT [Em Linha], 9.* https://www.aedb.br/seget/arquivos/artigos12/25416604.pdf

Linhares, J. E., Pessa, S. L. R., Bortoluzzi, S. C., & Luz, R. P. D. (2019). Capacidade para o trabalho e envelhecimento funcional: análise Sistêmica da Literatura utilizando o PROKNOW-C (Knowledge Development Process-Constructivist). *Ciência & Saúde Coletiva, 24*, 53–66. https://doi.org/10.1590/1413-81232018241.00112017

Lu, Q., Fu, C., Nan, K., Fang, Y., Xu, J., Liu, J., ... & Lee, B. G. (2023). Chinese corporate fraud risk assessment with machine learning. *Intelligent Systems with Applications, 20*, 200294. https://doi.org/10.1016/j.iswa.2023.200294

Magro, C. B. D., & Cunha, P. R. D. (2017). Red flags na detecção de fraudes em cooperativas de crédito: percepção dos auditores internos. *Revista brasileira de gestão de negócios, 19*, 469–491. https://doi.org/10.7819/rbgn.v19i65.2918

Mangala, D., & Kumari, P. (2015). Corporate fraud prevention and detection: Revisiting the literature. *Journal of Commerce & Accounting Research, 4*(1), 35–45. https://ssrn.com/abstract=2678909

Matar, D. O. (2023). Forensic accounting and Cybersecurity examine their interrelation in the detection and Prevention of financial fraud. *American Academic & Scholarly Research Journal*. https://www.aasrc.org/aasrj/index.php/aasrj/article/view/2209

Maulida, W. Y., & Bayunitri, B. I. (2021). The influence of whistleblowing system toward fraud prevention. *International Journal of Financial, Accounting, and Management, 2*(4), 275–294. https://doi.org/10.35912/ijfam.v2i4.177

Mohammed, A. F. A., & Rahman, H. M. A. A. (2024). The Role of Artificial Intelligence (AI) on the Fraud Detection in the Private Sector in Saudi Arabia. مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع, (100), 472–506.. https://doi.org/10.33193/JALHSS.100.2024.1018

Murphy, P. R., & Dacin, M. T. (2011). Psychological pathways to fraud: Understanding and preventing fraud in organizations. *Journal of business ethics, 101*, 601–618. https://doi.org/10.1007/s10551-011-0741-0

Nuswantara, D. A. (2020). Exploring Internal Control System As Deterrent To Occupational Fraud In Local Government. *SSRG International Journal of Economics and Management Studies, 7*(2), 103–114. https://doi.org/10.14445/23939125/IJEMS-V7I2P116

Özcan, A. (2019). Analyzing the impact of forensic accounting on the detection of financial information manipulation. *Manas Sosyal Araştırmalar Dergisi, 8*(2), 1744–1760. https://doi.org/10.33206/mjss.486662

Paiva, L. E. R. (2012). O presente e o futuro da dissuasão brasileira. In E. B. S. Filho, & R. F. Moraes. Defesa Nacional para o Século XXI: Política Internacional, Estratégia e Tecnologia Militar. *IPEA (Instituto de Pesquisa Econômica Aplicada)*. https://www.ipea.gov.br/portal/images/stories/PDFs/livros/livros/livro_defesa_nacional_secxxi.pdf

Pearson, T. A., & Singleton, T. W. (2008). Fraud and forensic accounting in the digital environment. *Issues in accounting education, 23*(4), 545–559. https://doi.org/10.2308/iace.2008.23.4.545

Pinheiro, G. J., & Cunha, L. R. S. (2003). A importância da auditoria na detecção de fraudes. *Contabilidade Vista & Revista, 14*(1), 31–47. https://revistas.face.ufmg.br/index.php/contabilidadevistaerevista/article/view/210

Prenzler, T. (2019). What works in fraud prevention: A review of real-world intervention projects. *Journal of Criminological Research, Policy and Practice, 6*(1), 83–96. https://doi.org/10.1108/JCRPP-04-2019-0026

PwC Brasil. (2022). *Protegendo o perímetro: o avanço da fraude externa*. Pesquisa Global sobre Fraudes e Crimes Econômicos, 2022. https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2022/pesquisa-global-sobre-fraudes-e-crimes-economicos-2022.html#:~:text=As%20amea%C3%A7as%20externas%20est%C3%A3o%20aumentando&text=Essas%20s%C3%A3o%20algumas%20das%20conclus%C3%B5es,dos%20fraudadores%20externos%20est%C3%A1%20crescendo

Ribeiro, A. M. (2014). Poder discricionário do gestor e comparabilidade dos relatórios financeiros: uma análise dos efeitos da convergência do Brasil às IFRS. [Doctoral dissertation, Universidade de São Paulo]. *Digital Library USP*. https://www.teses.usp.br/teses/disponiveis/12/12136/tde-10062014-171046/en.php.

Richmond, E. M., & Okoye, E. I. (2019). Empirical analysis of the relevance of forensic accounting as panacea to fraud detection and prevention in nigeria. *International Journal Multidisciplinary Research (IJMR), 5*(3), 60–66. https://eprajournals.com/IJMR/article/1279

Rosnidah, I., Johari, R. J., Hairudin, N. A. M., Hussin, S. A. H. S., & Musyaffi, A. M. (2022). Detecting and preventing fraud with big data analytics: Auditing perspective. *Journal of Governance and Regulation*, *11*(4), 8-15. https://doi.org/10.22495/jgrv11i4art1

Rossi, A. A., & Silva, P. R. D. O. (2016). O papel da auditoria interna para prevenção de fraudes nas empresas. *Revista Executive On-Line, 1*(1), 105–119. https://unifafibe.com.br/revistasonline/arquivos/revistaexecutiveonline/sumario/43/06012017180121.pdf

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. https://doi.org/10.1108/JAOC-09-2019-0098

Ruzgas, T., Kižauskienė, L., Lukauskas, M., Sinkevičius, E., Frolovaitė, M., & Arnastauskaitė, J. (2023). Tax Fraud Reduction Using Analytics in an East European Country. *Axioms, 12*(3), 288. https://doi.org/10.3390/axioms12030288

Samagaio, A., & Diogo, T. A. (2022). Effect of computer assisted audit tools on corporate sustainability. *Sustainability, 14*(2), 705. https://doi.org/10.3390/su14020705

Samuel, O. A., & Augustine, A. A. (2022). Internal Audit Efficiency and Fraud Prevention: Empirical Study of Listed Manufacturing Companies in Nigeria. *International Journal of Management and Economics Invention, 8*(9), 2631–2641. https://doi.org/10.47191/ijmei/v8i9.04

Santos, H. D. C., de Aragão Lourenço, G., Pereira, M. D., & Boreli, D. (2023). A importância da auditoria interna na detecção de fraudes tributárias: um estudo exploratório sobre a percepção dos profissionais da área. *Razão Contábil e Finanças, 14*(1). https://periodicos.uniateneu.edu.br/index.php/razao-contabeis-e-financas/article/view/317

Santos, L. M. L., de Souza, D. V. B., Vasconcelos, O. I., & Roberto, J. C. A. (2021). Controle interno como ferramenta de gestão na prevenção e redução de fraudes e erros nas organizações empresariais Internal control as a management tool in the prevention and reduction of fraud and errors in business organizations. *Brazilian Journal of Development, 7*(10), 99169–99185. https://doi.org/10.34117/bjdv7n10-301

Silva, J. V. (2022). Auditoria contábil e suas contribuições para o processo de gestão nas organizações empresariais. [Projeto de Conclusão de Curso, Faculdade Pitágoras]. *Repositório Pitágoras.* https://repositorio.pgsscogna.com.br/bitstream/123456789/44644/1/JO%C3%83O_VITOR_DA_SILV.pdf

Silva, K. H. A., do Nascimento, J. C. H. B., de Sousa, W. D., Bernardes, J. R., & da Silva, F. C. B. (2015). O controle interno na prevenção de fraudes: um estudo de caso numa mineradora. *Revista Opara, 5*(1). https://research.ebsco.com/c/spunt7/search/details/vuei27z5yz?db=iih

Silva, M. R., Hayashi, C. R. M., & Hayashi, M. C. P. I. (2011). Análise bibliométrica e cientométrica: desafios para especialistas que atuam no campo. *InCID: revista de ciência da informação e documentação, 2*(1). https://doi.org/10.11606/issn.2178-2075.v2i1p110-129

Simanungkalit, J. A. R., Hertadi, R., & ul Hosnah, A. (2024). Analisis Tindak Pidana Penipuan Online dalam Konteks Hukum Pidana Cara Menanggulangi dan Pencegahannya. *AKADEMIK: Jurnal Mahasiswa Humanis, 4*(2), 281–294. https://doi.org/10.37481/jmh.v4i2.754

Simmons, M. R. (1995). Recognizing the elements of fraud. *The Fraud Magazine.*

Singh, N., Lai, K. H., Vejvar, M., & Cheng, T. E. (2019). Data-driven auditing: A predictive modeling approach to fraud detection and classification. *Journal of Corporate Accounting & Finance*, *30*(3), 64–82. https://doi.org/10.1002/jcaf.22389

Solomon, A. N., Emmanuel, O. O., Ajibade, D. S., & Emmanuel, D. M. (2023). Assessing the effectiveness of internal control systems on fraud prevention and detection of selected public institutions of Ekiti State, Nigeria. *Asian Journal of Economics, Finance and Management*, 231–244. https://journaleconomics.org/index.php/AJEFM/article/view/211

Tariq, E., Akour, I., Al-Shanableh, N., Alquqa, E., Alzboun, N., Al-Hawary, S., & Alshurideh, M. (2024). How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks. *International Journal of Data and Network Science, 8*(1), 69–76. https://doi.org/10.5267/j.ijdns.2023.10.016

Tatineni, S. (2020). Enhancing Fraud Detection in Financial Transactions using Machine Learning and Blockchain. *International Journal of Information Technology and Management Information Systems (IJITMIS), 11*(1), 8-15. https://iaeme.com/Home/article_id/IJITMIS_11_01_002

Ubesie, M. C., Ibezim, N., & Cyriacus, M. (2023). The Impact of Internal Control Measures on the Detection and Prevention of Fraud in Banks (A Case Study of Fifteen (15) Selected Deposit Money Banks in Nigeria). *International Journal of Banking And Finance Research, 9*(1), 24–37. https://doi.org/10.56201/ijbfr.v9.no1.2023.pg24.37

Wells, J. T. (2004). New approaches to fraud deterrence. *Journal of Accountancy New York, 197*(2), 72–76. https://www.journalofaccountancy.com/issues/2004/feb/newapproachestofrauddeterrence/

Wicaksono, D., & Yuhertiana, I. (2020). Case Study: Evaluation Of Fraud Control Plan (Fcp) Attributes As Fraud Prevention Tool. *E-Prosiding Akuntansi*, *2*(2).

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. [Faculty Publications, Kennesaw State University]. Kennesaw State University Library System. https://digitalcommons.kennesaw.edu/facpubs/1537/

Zhang, Y., Hu, A., Wang, J., & Zhang, Y. (2022). Detection of fraud statement based on word vector: Evidence from financial companies in China. *Finance Research Letters, 46*, 102477. https://doi.org/10.1016/j.frl.2021.102477

CONFLICT OF INTERESTS

The authors declare no conflict of interest regarding this submitted work.

AUTHOR CONTRIBUTIONS

Roles	1st author	2nd author
Conceptualization	♦	♦
Data curation	♦	♦
Formal analysis	♦	
Funding acquisition		
Investigation	♦	
Conceptualization	♦	♦
Project administration		
Resources		
Software		
Supervision		♦
Validation		♦
Visualization	♦	
Writing – original draft	♦	
Writing – review & editing		♦