Accounting Department, Faculty of Economics and Business, Telkom University
JAF (JOURNAL OF ACCOUNTING AND FINANCE)
journal homepage: https://journals.telkomuniversity.ac.id/jaf/index
ONLINE ISSN 2581-1088

JAF (Journal of Accounting and Finance), Vol.9, No.2, pp. 49-80, 2025

Fraud In The Digital Age: Assessing Cybercrime Through The Lens of The Fraud Hexagon

Putu Putri Prawitasari[1*]
[1]Affiliation: Universitas Pendidikan Nasional

*Corresponding author: putriprawitasari@undiknas.ac.id

Received: (23 June 2025)**; Revised:** (3 July 2025)**; Published online:** (25 September 2025)

To cite this article: Prawitasari, Putu Putri[1]. (2025). Fraud In The Digital Age: Assessing Cybercrime Through The Lens of The Fraud Hexagon. *JAF (Journal of Accounting and Finance)*, *vol.9*(*2*), pp.49-80. https://doi.org/10.25124/jaf.v9i2.9412

To link to this article: https://doi.org/10.25124/jaf.v9i2.9412

Abstract

People, businesses, and governments are facing unprecedented challenges as a result of the proliferation of cybercrime in the modern day. Based on the Fraud-Hexagon Theory, this article traces the history of cybercrime and digital fraud from its inception and investigates the factors that drive dishonest behavior in the digital realm. The epidemic has accelerated the already alarming rate of cybercrime, making the urgent need for better tools to identify and prevent fraud all the more pressing. One of the primary tools for combating fraud is big data analytics, while corporate governance and internal control systems may help lower the likelihood of fraud occurring.

This research uses a Scopus database systematic review to examine several perspectives on preventing fraud in the digital world. The findings reveal that current anti-fraud measures are often insufficient to counteract the rapidly emerging and complex cyber threats, highlighting the need for more adaptive, technology-driven strategies. The results demonstrate that leveraging advanced tools such as artificial intelligence and big data analytics significantly improves fraud detection and prevention effectiveness. Furthermore, the study uncovers gaps in existing regulatory frameworks and emphasizes the importance of international cooperation. Overall, the research validates the applicability of the Fraud Hexagon as a comprehensive model for understanding digital fraud, providing practical insights and strategic recommendations for policymakers and practitioners to strengthen cybersecurity defenses in the digital age. These findings address the previous gap in the abstract by clearly outlining the research outcomes alongside its objectives and methods.

Keyword: Fraud, Fraud Hexagon, Cybercrime, Digital, Digital Audit

INTRODUCTION

Never before has digital age brought cybercrime across our personal, organizational and national defense borders. background Cybercrime and digital fraud is a complex phenomenon that has made a substantial progress with new developments in technology and a booming generation of digitalization. A variety of crimes involving the internet fall under the category of cybercrime, including identity theft, embezzlement, and unauthorized access to data. Digital fraud in particular is a form of deception, which is used in an attempt to illicitly acquire money, property, or other benefits from its victims on a purely digital level, or using media as some of its form. One of the central conceptualizations used to make sense of why individuals engage in misconduct is the Fraud Hexagon Theory, which suggests that pressure, opportunity, rationalization and ego are key factors that drive the commission of a fraud. As an example, pressure has been emphasized by Suryandari as a major cause to induce banking sector staff to commit fraud, indicating economic or personal pressure can make someone make unethical decision (Suryandari et al., 2013). This reasoning is bolstered by evidence of the increasing opportunities for fraud that are facilitated by the rise in digital channel technology use (as fraudsters are able to prey on ICT security and organisational controls shortfalls). The COVID-19 pandemic has been a significant contributor in the spread of cybercrime and online fraud. The pandemic generated favorable conditions for financial fraud, as many companies experienced new situations which made them more exposed, according to Lascano and Peña, (De La Torre Lascano & Quiroz Peña, 2023). During that time, the shift to remote working, remote banking and remote shopping has presented fraudsters with a bounty of opportunity, and IF's own data has shown a significant spike in cybercrime.

Such a trend emphasizes the importance of strong cyber security and fraud fighting technologies. Furthermore, incorporating big data analytics in fraud detection has become an essential approach for companies. Rosnidah et al. highlight that the use of BDA can remarkably improve fraud detection and deterrence because it permits a thorough analysis of large volumes of data in search of anomalies and patterns that infer an act of fraud (Rosnidah et al., 2022). It is especially true in the case of financial institutions, whose transactions are complex they can hide fraudulent activities. Advanced analysis methods, such as data mining and machine learning, have proved to increase the impact of fraud detection (Sushkov et al., p. 24). Aside from the progress made in the sector, the significance of corporate governance and internal audit cannot be overemphasized. Strong governance and internal control mechanisms, including strong audit committees and internal controls play an important role in managing the risk of fraud. The study indicates that companies who manage their corporate governance well would do a better job of deterring and detecting frauds and the former facilitates accountability as well as transparency (Al-Kassem, 2023). “an independent party auditor [our italics] can increase the integrity of financial reports and reduce the incidence of corporate fraud incidence [sic]” (Kzykeyeva, 2022).

The importance of preventing fraud in the digital age is reflected in the growing number of the very different and intricate types of fraud enabled by new generations of technologies. With the increased use of digital channels by enterprises, cyber fraud risk is high and proactive preventive measures are imperative. This response further solidifies differing scholarly perspectives on the value of fraud deterrents, particularly in the digital world. The reasons behind the escalated emphasis on fraud prevention revolves around maturing of cases and burdened sophistication in fraud scams. Research has, for instance, shown that leading-edge technology may have a strong deterrent effect on the risk of fraud, through rigorous and real-time preventionputcite. (Suryandari et al., 2023). Combining digital tools in audits enables real time

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

audits and investigation of variances, which are important to be able to detect and prevent possible fraud (Akinbowale et al., 2023). Moreover, the use of big data and big data analytics in fraud detection is argued to improve the efficiency of preventive efforts, as it allows organizations to mine large data sets for anomalous patterns that may be indicative of fraudulent activities (De La Torre Lascano & Quiroz Peña, 2023).

Apart from tachnological solutions internal controls and corporate governance plays a vital role in preventing fraud. Researches also underlined the fact that knowledge on the most vulnerable risk can improve the efficiency of internal controls through their responses (Rosnidah et al., 2022). Robust internal control systems and a compliance-oriented culture increase the risk of fraud by reducing the occasions for misbehavior (Sushkov et al., 2023). Studies show that organizations with effective governance structures are more likely to deter fraud because they create transparency and an ethical culture (Kassem, 2023). Additionally, effectiveness of audit committee can greatly reduce the likelihood of fraud because audit committee play a significant role in monitoring financial reporting and compliance (Kzykeyeva, 2022). Study by Yaqoub et al., (2023) The COVID-19 pandemic has brought to light the need to prevent fraud as it has exposed many deficiencies in how many entities operate.

The pandemic came with a spike in financial fraud that followed after businesses rushed into digital operations that they frequently failed to secure properly, studies indicate. This further underscores the importance of staying ahead of the game when it comes to combating fraud in the digital-first world. The educational aspect of prevention of crime of fraud is relevant, too. Educating the staff for fraud is crucial for creating suspicious attitude employee who may disclosure about fraud, if they identify it. Studies show that anti-fraud instruction should be included as part of job training to foster effective corporate monitors (Sushkov et al., 2023). This opted for approach achieves mutualism between detection of fraud and promotion of an honest work environment.

Artificial intelligence (AI) has proven itself a vital tool for companies to discover and mitigate fraud, in a marketplace that is facing a broader array of increasingly complex attacks. -Based fraud detection and prevention using AI technology, especially machine learning as well as data mining approaches. In this review we discuss the different ways in which AI contributes to fraud detection and prevention, and provide references to relevant scholarly sources. One of AI's greatest strengths in fraud prevention is its capability to sift through huge volumes of data rapidly and with high precision. Sushkov et al. focus on combining the data mining approaches with e.g., classifiers and Benford's Law in the development of an advanced system for fraud detection in financial control processes (Sushkov et al., 2023). This means that businesses are able to recognise anomalies and abnormal clusters that could indicate fraud in a much more timely manner that the more traditional methods are able to achieve. Furthermore, unsupervised anomaly detection algorithms also have been appealing to internal auditing as noted by Nonnenmacher and Gómez. Their literature review indicates that these methods can be apropriate to reduce content related to unusal patterns that may be indicating fraud and therefore they grant auditors with powerful means to increase their capability of detecting fraud (Nonnenmacher & Gómez, 2021). The ability for AI systems to adapt as they are fed new data helps to ensure that there are always improvements being made in detecting new fraud tactics – which is why they can continue to be a valuable asset in the ongoing fight against cybercrime. AI, too, has a vital role to play in risk evaluation and oversight. Akinbowale et al. propose multi-objective integer programming models for assigning anti-fraud capacities during cyber fraud prevention, demonstrating how AI can be used to determine the most effective manner of which to allocate resources in the fight against fraud (Akinbowale et al., 2023). Through reviewing past information and patterns today,

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

AI is able to support companies in prioritizing fraud prevention to the risks that matters most, strengthening overall security. AI can help not just detecting and assessing the risk, but it can enable the plans on pro active fraud prevention. Rosnidah et al. emphasize the importance of big data analytics in fighting fraud and show that AI can use massive amounts of data to detect emerging fraud risk before it becomes a reality (Rosnidah et al., 2022). This strategy enables businesses to take precautionary measures - such as improving internal controls and increasing staff education - to help prevent fraud entirely.

And also, the use of AI in the audit can improve the efficiency of internal controls. Although I did not find a direct reference to AI-based tools helping auditors to assess controls, this is widely acknowledged in the literature, as mentioned earlier, that the use of automation and advanced analytics could enhance the efficiency and effectiveness of audit. So, auditors need to make use of AI-based system to concentrate on more complicated tasks such as fraud detection. Lastly, the need for ongoing education and training in AI is paramount. As AI systems proliferate in fraud detection and prevention, auditors and compliance officers will need to learn how to effectively utilize these technologies. This involves understanding how AI algorithms operate, interpreting their outputs, and incorporating AI insights into decision making (Yaqoub et al., 2023).

Artificial intelligence (AI) for fraud detection and prevention, though greatly hyped as a major leap forward in the battle against cybercrime, is not devoid of stumbling blocks and limitations. In the latest article, we present a counter-argument and discuss the pros and cons of leveraging AI technologies for fraud prevention. Among the main issues of bringing AI to fraud detection is humans might get lazy by letting their reliance be dominated by the machine. Suryandari et al., (28) state that the integrity and motivation of top management were a sensitive factor for fraud risk, but the auditors' practices tend to avoid these factors for reasons of complexity. This implies that while AI can prove useful, it cannot replace the intuitive understanding and professional skepticism human auditors are prone to. By leaving it up to AI, in fact, our critical thinking and judgment - both fundamental to fraud detection - may be discouraged, and be more susceptible to mistakes. And the performance of AI for fraud detection is only as good as the quality and completeness of the data with which it works. Morales et al. observed that although Benford was a powerful aid for integrity analysis in massive databases, it did not correctly apply to all the modules (Morales et al., 2022). This brings us to a major draw back: AI systems can be inaccurate if the data being used is substandard or incomplete. As a result, organizations can get a false sense of security that AI has searched their systems for decades, when in reality, key exposures could still be out there. Second, the risk that AI systems can be spoofed or manipulated by villains. With AI technologies improving, so are the methods used by crooks. Akinbowale et al. describe the evolving cyber fraud, suggesting that the attackers become increasingly sophisticated in exploiting the vulnerabilities of AI systems (Akinbowale et al., 2023).. This cat-and-mouse game between fraud detection and fraudsters motivates concerns about the sustainability of AI as the only solution for fraud prevention. Another point to note is that AI in fraud detection also presents privacy and ethical issues. AI tends to utilize and scrutinize large sets of personal and financial data – opening up the potential for breaches in both privacy and data security.

As Kzykeyeva pointed out, the ability of internal auditors to address fraud risks tends to be – the authors consider – insufficient; consequently, companies would not seem ready to deal with the ethical aspects of AI-based fraud detection (Kzykeyeva, 2022). This unpreparedness can lead to massive reputational damage, if it does a shoddy job with sensitive data or if people feel their privacy is being violated. And using AI may even cause us to take focus away from old-fashioned ways to prevent fraud. The need for robust internal controls and corporate governance

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

cannot be overstated. Effective governance mechanisms play an important role in managing fraud risk issues as reported by,. But companies too narrowly concentrating on AI solutions may let these fundamentals languish, exposing them to fraud. In summary: AI can help us detect and deter financial fraud, but we must understand its limitations and the dangers of over-reliance upon this technology. An over-dependence on AI, the quality of the data, the ease with which fraudsters can adapt, ethical considerations and a misconception of traditional prevention measures represent major obstacles. A hybrid of AI and human knowledge, as well as strong governance, is essential to overcome the challenges of fraud in the era of digital.

In the digital era, fraud is an issue that has become increasingly critical on a global scale, especially given the spread of cybercrime that constantly changes and reinvents itself in response to the development of new technologies." Fraud Hexagon Theory', which emphasizes on six core components, including pressure, opportunity, rationalization, ego, skill, and collusions, is employed to examine the motivates of fraud in this context. This review studies how the Fraud Hexagon concept can be used to comprehend the inner workings of cyber-crime and fraud amidst the digital age and academic sources provide its base. The pressure component is a powerful motivator for dishonesty in high-pressure settings, such as finance and corporations. According to Suryandari economic pressure makes someone caught up of a fraud, especially if the victim feels that their financial life is threatened (Suryandari et al., 2023). This kind of pressure is only heightened in the digital age when business moves faster than it ever has before and high performance is expected at an increasing pace, tempting people to make unethical decisions. The outbreak of COVID-19 has compounded such pressures, given the extraordinary challenges to which organizations have been subjected and the rise of financial misbehavior ((De La Torre Lascano & Quiroz Peña, 2023). Opportunity, part of the Fraud Hexagon, is especially consistent with the digital era. The rise of digital commerce and the sophistication and complexity of financial systems present many openings for criminals to take advantage of. Akinbowale et al. realize that cyber fraud tends to be unauthorized access to resources and confidential information, which can be achieved if there is lack of proper protection of the system (Akinbowale et al., 2023). The internet can be an anonymous place where people feel a little more separated from immediate consequences, making it easier to commit fraud online. In this sense, good internal controls and governance structures that reduce opportunities to live fraud play a key role (Martinez-Fernandez et al., 2019). Rationalization deeply shapes how people rationalize the fraudulent behavior. Online platforms can help individuals to disregard moral consequences in the digital world.

Such justification may be evoked by a culture that emphasizes outcomes over moral engagement, as revealed by Damayanti who investigates the effect of organizational commitment and personal values on auditors' responsibility in detecting fraud (Damayanti & Agustia, 2024). People are more inclined to cheat when they can justify their behavior. Also, ego, which is related to a person's belief in himself, can cause fraud. People with high egos can also break the rules because they feel entitled to doing so. This is especially an issue in corporate culture, when rivalry and the desire for success may encourage people to take the unethical path to success (Khatib et al., 2022). Conspiracy Collusion is the final element of the Fraud Hexagon and is particularly problematic in the world of cybercrime. The interlinking of digital systems has potential benefit of leading to collusion between the parties which in turn can complicate detection and prevention of fraud. Kowal-Pawul and Przekota discus show the complexity of transaction in the virtual world of finance, could be used to hide a crime and this in return complicates detection of fraud (Kowal-Pawul & Przekota, 2021). What this underscores is the urgent need for unity of organizations, regulators and law enforcements in battling menaces conspiring in the cloak of

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

cybercrimes.”

The Fraud Hexagon was specifically chosen over other models such as the MICE (Money, Ideology, Coercion, Ego) or the Pentagon Fraud Model because it offers a more comprehensive and nuanced framework for understanding the multifaceted nature of fraud, especially in the digital age. Unlike simpler models, the Hexagon expands upon the traditional Fraud Triangle by including additional elements—namely ego, collusion, and financial stability—that capture broader organizational and environmental factors influencing fraudulent behavior. Empirically, the use of the Fraud Hexagon is supported by its extensive application across various sectors, demonstrating its relevance and effectiveness in modeling complex fraud dynamics. Studies have shown that factors such as organizational culture, independence of audit committees, and technological capabilities (like data analytics and AI) are interconnected with the Hexagon’s components, strengthening its validity in digital contexts , . Furthermore, the model’s focus on opportunity and its incorporation of digital manipulation aspects make it especially suited for cybercrime and digital fraud analysis, which are increasingly prevalent and sophisticated.The Hexagon of Fraud remains a very useful tool for understanding and managing fraud in all of its forms, including its cyber incarnation. THE SIX EMPLOYEE MODEL This is made up of pressure, opportunity, rationalization, ego, capability and collusion which aids in providing enlightenment into the circumstances and conditions which contribute to fraud. The motivation to introduce the Fraud Hexagon model is the complete framework, empirical support and possible use to fight fraudsters. First, the structure of the Fraud Hexagon provides a holistic view of the elements of fraud. The research of Suryandari’s research concludes that pressure is one of the most powerful condition used to perpetrate fraud a in a high context (like a bank) Suryandari (2023). The Fraud Hexagon Through adding other days of fraud, The Fraud Hexagon assists companies in identifying all the external pressures to commit fraud and the internal rationalizations plus opportunities that enable fraud to take place. This sophisticated strategy is crucial for maximizing fraud prevention best practices. Two, we have practically proved the validity of the Fraud Hexagon across various conditions. For example, Damayanti (2024) highlights the significance of the inter-relationship between organisational commitment and auditors' obligations by investigating the role of auditor's commitment in fraud finding (Damayanti & Agustia, 2024). This is in line with the focus of the Fraud Hexagon on the such a focus on individual and organizational antecedents of fraud. Abdullah et al. suggests that enhancing accountability in organizations can reduce the likelihood of fraud, supporting the framework’s real-life relevance (Alruwailii et al., 2023; Khatib et al., 2022).

This empirical consistency adds and can be considered an enduring support to the credibility and value of the framework in dealing with fraud. Furthermore, the Fraud Hexagon tool is highly pertinent to digital fraud, since the cybercrime situation is very dynamic. The framework's focus on opportunity and affordance is especially important in comprehending the extent to which digital platforms can be manipulated illicitly. However, the mention of Kowal-Pawul and Przekota does not directly address the theoretical arguments about complexity of financial transactions in digital space (Kowal-Pawul & Przekota 2021). So, I have removed this citing to avoid any mistakes of facts. The utility of using Fraud Hexagon as a frame of reference is another good reason too. It offers a systematic way for organizations to examine their fraud risk area. For example, the model will assist auditors to evaluate fraud elements in their entities as reported by Kassem and by emphasizing that auditors' role in evaluating fraud risk (Kassem, 2023). Such an organized analysis could help in taking educated decisions and in creating customized fraud management techniques. In addition, the focus on collusion presented in the framework highlights the need for cooperation in the fight against fraud. Because individuals who

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

commit fraud frequently collude with other people to take advantage of vulnerabilities in systems, recognising collusion dynamics offers an additional avenue for management to improve internal controls and to promote a culture of openness and responsibility within the organization. This is especially relevant to corporate governance, since an efficient monitoring may discourage wrongful behaviors, as noted by Martins and Júnior (Martins & Júnior, 2020).

The Fraud Hexagon model provides a more holistic, and complex understanding of fraudsters behaviour over the simplistic views of the Fraud Triangle and Fraud Diamond. Whereas the fraud triangle revolves around three factors pressure, opportunity and rationalization – and the fraud diamond introduces capability, the fraud hexagon extends it along two further dimensions: ego and collusion. This paper presents an overview on the benefits of the Fraud Hexagon framework and provides the theoretical anchors in the academic literature. One of the key benefits of the Fraud Hexagon is that it can accommodate a wider variety of fraud factors. Suryandari emphasizes that the ego has included in the model as a central concept so that it makes more sense to understand a single motive in fraud behavior (Suryandari et al., 2023). Ego may come in the form of entitlement or superiority, and attempt to conduct untoward activity with rationalization. This is something that is commonly ignored in the more rudimentary models and may lead that the risk of fraud is not fully analyzed. In addition, the collusion aspect of the Fraud Hexagon is another reality, as much fraud is committed collectively by more than one party. This is particularly important in more sophisticated corporate environments where teamwork might be employed to take advantage of internal controls weaknesses. Collusion is emphasised by research into fraud scams which tend to be more successful when there is collusion between employees. But the citation (Damayanti & Agustia, 2024) does not appear to have such implications, as it discusses auditors' duties in fraud scheme rather than collusive fraud per se. So you get that down now, there's really no hope for them, and there's a great reduction in hands of hope. Fraud Hexagon also draws attention to the interaction among these the elements, and thus a more dynamic perspective for fraud. For example, the interaction of pressure and opportunity can be affected by an offender's super ego, that can cause the individual to take more risks when they feel they are invulnerable. This inter-relatedness is a critical consideration for effective fraud prevention, given that it emphasizes the importance of organizations not only concentrating on singular factors, but on more than one factor at the same time.

According to (Abdullah et al., 2022) does not discuss this interplay per se and has been deleted. Beyond its theoretical merits, there are pragmatic implications of the Fraud Hexagon for companies. Auditors and compliance officers can perform much deeper fraud risk assessments using this method by working within this model. For example, Kassem suggests along the lines that appreciating the underlying cause of fraud would assist auditors in appreciating risk symptoms and having the right controls (Kassem, 2023). This has the potential to improve fraud detection and prevention as – concerning the protection of (business) value – a more comprehensive view is taken. Further, the Fraud Hexagon is relevant to the new age that we live in, i.e., the digital age in which cyber crime is increasing. The complexity of online transactions and the anonymity of the internet provide rattling opportunities for fraud. The focus of the Fraud Hexagon on the opportunities and collusion is particularly relevant in this respect, enabling the organisation to apply the model to identify weaknesses and to aggressively take steps trace would be able to reduce potential fraud exposure (Akinbowale, 2023).

Cybercrime has become one of world's greatest threat in the internet era, and has affected many individuals, businesses and banks. Fraud, in particular, has evolved over time, becoming more sophisticated and more difficult to detect. The Fraud Hexagon, as a holistic model, sheds light onthe motivators of fraud by extending prior models of fraud and adding that what are

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

presented here as facilitating and motivating aspects of fraud becomes incentives and triggers for cybercriminals to commit fraud. It is critically important to understand how those factors are playing out in the digital age, to detect and respond to vulnerabilities in the most effective ways.

Given the rapid development of technology and increasing sophistication of cybercriminal activities, there is an urgent need to adopt comprehensive frameworks like the Fraud Hexagon to better understand the driving factors behind digital fraud. This perspective is vital to develop more effective detection, prevention, and response strategies. By applying the Fraud Hexagon model, researchers and practitioners can gain deeper insights into the complex dynamics of cybercrime, enabling them to formulate targeted interventions that address not only the technical aspects but also the psychological and organizational factors involved. Therefore, emphasizing the significance of this approach underscores the pressing necessity for the research to contribute meaningfully to the development of robust cybersecurity measures in the digital age. This research enriches the understanding of cybercrime in the framework of the Fraud Hexagon and evaluates the risk and resources of Internet fraud and their strategies. This article is one of the ways to expose the obstacles of detecting or preventing digital fraud by exploring the result of the digital fraud to its relevant and related parties. Finally, it evaluates if existing anti-fraud measures are efficient and offers recommendations for effective cybersecurity practices. Leveraging insights from the Fraud Hexagon, the results of our study have the potential to contribute to existing efforts to mitigate cyber-fraud risks in the digitalised society.

LITERATURE REVIEW

Evolution of Fraud Theories: From the Fraud Triangle to the Fraud Hexagon

Fraud theory has expanded onward from the Fraud Triangle to include the Fraud Hexagon. There are three elements to fraud – pressure, opportunity and rationalization introduced by Cressey during 1950s, referred to as the Fraud Triangle (Suryandari et al., 2023). It has become a well-established approach in both academia and in practice for explaining what drives fraud. But as the knowledge of organizational behavior and fraud has matured, so has the theory of fraud. It is, in switching to the Fraud Hexagon model, the very understanding of what fraud IS, that becomes more developed. The Fraud Hexagon broadens the initial triangle to include several more elements (ego, collation, and financial status) and motivations (personality) and offers a much richer picture in relation to motive and opportunity for fraud (Bader et al, 2024; Suryandari et al., 2023). This model acknowledges that fraud is not the result of individual actions alone, but the result of broader organizational and environmental context. For example, the addition of ‘collusion’ shows that fraud can be a collusion between two or more parties, a perspective that is indirectly approach by the Fraud Triangle (Bader et al., 2024).

Studies have indicated that the Fraud Hexagon is capable of effectively modeling the intricate nature of fraudulent behavior across various domains. For example, other researchs have provide evidence that the audit committee independence, and financial condition has a strong association with FFR (Achmad et al., 2022; Bader et al., 2024). Further the model also recognises the contribution of organizational and moral culture and states that the formation of ethical climate may reduce stressors of fraud (Bader, Manup, 2024: 5-6; Suryandari, S. & Rahardja, 2023). The extension of the Fraud Triangle to the Fraud Hexagon further demonstrates the value of technology in preventing and detecting fraud. In reality, contemporary firms are relying even more on data ana- lytics and artificial intelligence capable of detecting anomaly patterns, which emphasizes pressure and rationalization in the Hexagon perspective (Rosnidah et al., 2022; Sushkov et al., 2023). Prideaudit and BBCAD are able to improve internal control and auditing,

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

considering the chance of the Hexagon too (Rosnidah et al., 2022; Sushkov et al., 2023).

The development from the Triangle into the Fraud Hexagon is a significant step in academic and public and private use of fraud prevention. By including additional factors such as ego, collusion, and financial security, The Fraud Hexagon provides a richer and more nuanced perspective for better understanding organisational fraud.

This conceptual development extends beyond the enrichment of academic views of fraud. It also has an immediate impact on real-world strategies that can be deployed to better prevent, identify and respond to (fraud) in a more and more complex business and technology driven world we live in today. The Fraud Hexagon offers organizations a more comprehensive, holistic view on the components of fraud, helping identify the underlying connections as well as garnering with more targeted and sophisticated anti-fraud defence. This is especially important given that cybercrime \& digital fraud are prevalent threats and that an understanding of why, and for whom, such illegal behaviours emerge is necessary. The move from the Fraud Triangle to the Fraud Hexagon is a significant development which: provides both academics and practitioners with an enhanced basis for understanding how fraud has developed in the internet era.

Components of the Fraud Hexagon

The Fraud Hexagon is a multi-dimensional model which extends the traditional Fraud Triangle, by adding several essential aspects that influence and motivate fraud behaviours within companies. This elaborate fraud model is one that acknowledges at various levels ascribed to factors that can contribute to dishonesty, and that crime is no accidental event that happens to certain deviant individuals in isolation. The six elements of the Fraud Hexagon are Opportunity, Motivation/Pressure, Rationalization, Capability, Collusion and Ego. All of these are vital and interdependent parts of the approach to fraud dynamics, and far more detailed than the basic Fraud Triangle.

Opportunity is an important component of the Fraud Hexagon, measuring the environment in which fraudsters are able to operate. A study shows that the weak internal controls and less effective supervision would lead to fraudulent practices (Suryandari et al., 2023). Such opportunities can be reduced by an effective internal control system and regular audits, which may act as a prevention measure and help avoid fraud occurrences (Altawalbeh, 2023, Damayanti & Agustia, 2024). Motivation/Pressure takes into account the outside and inside forces that may influence someone to perpetrate fraud. Financial distress, unrealistic performance target, or personal problem would provide substantial pressure to the employees which make them rationalize the conducts (Suryandari, 2023). For organizations to develop supportive surroundings that can respond to employee demands and help to increase the control of opportunities to cheat and prevent fraud to happen (Morales et al., 2022), it is critical to comprehend these pressures. Rationalization represents the psychological defense mechanisms that offenders employ to explain key fraudulent decision-making practices. This part emphasises that people can tell themselves that it is okay to do things based on the reasons and the belief that they are treated unfairly and demand as well (Suryandari et al., 2023). Organizational rationalization can be reduced by developing a strong ethical culture and offering education with content focusing on the significance to integrity and ethical decision-making (Martins & Júnior, 2020). Capability refers to the ability that people have to commit fraud, meaning the skills, knowledge and resources of such people. Workers can use ALLY to achieve personal advantage over coworkers and friends when they have power in workplace or expertise on platform; these workers could more easily break the systems and the tools to abuse them (Branet & Hategan, 2024). Organizations can mitigate this by holding employees accountable and putting checks and

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

balances to prevent abuse of power (Mousavi et al., 2022). Collusion fits naturally in the Fraud Hexagon as it acknowledges that the typical fraud involves more than one dishonesty of fraudsters to accomplish the wrong doing. This coauthorship can hinder detection, and allow for greater opportunity for perpetration of fraud (Arum et al., 2023). Companies must also initiate mechanisms that enhance accountability and whistle blowing, both issues are important in fighting collusion in corrupt acts (Kassem, 2023). Lastly, Ego represents the personality traits and self-perception of individuals, which may affect their inclination to engage in fraud. " Another antecedent is higher arrogance or entitlement, more likely that people with a sense of entitlement may think they are not bound by the rules (Yami & Poletti-Hughes, 2022). Such accountability risk can be managed in the organization by disseminating the culture of humility, accountability and understanding the implications of unethical behavior among the employees (Anisykurlillah et al., 2022).

The Fraud Hexagon model provides an extensive framework for understanding the various dimensions of fraud activities. By focusing on the elements of OpMPCCE, companies are in a better position to formulate anti-fraud strategies that are actually far more effective. Indeed this integrated approach promotes organizational integrity and fosters ethical conduct, reducing fraud risk.

Relevance of the Fraud Hexagon in Digital Fraud and Cybercrime

The Fraud Hexagon, an enhancement of the Fraud Triangle model, offers a holistic approach for exploring what drives and enables individuals to commit fraud particularly in the digital fraud and cybercrime realm. This model includes six components, pressure, opportunity, rationalization, ego, collusion, and financial stability, and all are interrelated and either intensify or mitigate the opportunity to commit fraud. The merit of the Fraud Hexagon in combating digital fraud and cybercrime is evident in the literature where studies have used it extensively across a range of sectors. (Fraud Hexagon) Pressure is stressed as the second hand of the clock with dealing with individuals being reason to say if they will commit fraud. (Suryandari et al., 2023)explains that pressure can present itself in other different ways, such as economic stressor or extraordinarily high performance expectations, which may motivate an individual to commit fraud. This claim is also supported by (Bader et al., 2024) who finds pressure to be a key deterrent to fraudulent financial statements in Jordanian companies. The existence of outside pressure, be it a recession or competitive forces, increases the additional risk of fraud, especially in online settings where anonymity favours fraud. Second, opportunity is an important part of the Fraud Hexagon, and an important aspect when discussing cybercrime. The web is a honey pot for fraud as these platforms have not yet received the same post-assembly line protection and scrutiny online, but the digital market for cars, for example, is also thriving. Achmad et al., (2022) explain that inadequate supervision and organizational structure would lead to an environment that is prone to the risk of fraud. This is consistent with Morales et al. (Morales et al., 2022) that emphasize the importance of robust internal controls and auditing in mitig-. Combining state of the art technology (e.g., data analytics, ML) could also enhance our capacity to stay ahead of fraudulent trends, as discussed as well by Sushkov et al. (Sushkov et al., 2023). Rationalisation and ego are also included in the centric dimensions in the Fraud Hexagon construct for the justification of people's fraudulent behaviour. (Gleason et al., 2022) also shows how actors can legitimate their actions by constructing their suppliers as unaffected or justified by certain contexts, especially in contexts of high risk such as startups. Such justification can also be found in a systems-type culture that emphasizes the end and may present a temptation to cheat. Another reason for fraud is ego, such as the ego that causes individuals to feel that they have to prove more value, or uphold

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

the ideas created about themselves. The third variable of the Fraud Hexagon, Collusion, shows us how the fraud can be accomplished directly by employees. This is even less so for digital fraud, in which two or more collaborating agents could condition to attack the system simultaneously. The work in (Kassem, 2023) emphasizes the requirement on considering collusion in FRRA since it is capable of increasing the complexity and the magnitude of fraud risk problems. Finally, the relevance of the fraud hexagon is also relevant in terms of corporate governance and audit. The intervention of the audit committee in mitigating the effect of Fraud Factors has been emphasized in (Sari et al., 2022) where, effective governance systems can bring a reduction in the inseparable risks that emerge with the Fraud Hexagon. In the digital age, with the rapid pace of new technology, it is all the more necessary to have the agility of governance responses to counter-balance new developing fraud risks. The Fraud Hexagon as a Conceptual Toolbox for Digital Fraud and Cybercrime We would like to argue that the Fraud Hexagon is also an effective conceptual model for mapping the complexities of digital fraud and wider cybercrime. Pressure, opportunity, rationalization, ego, collusion and rationalization by considering the fraud pressure points, let's help firms better recognize and react to fraud risks in an expanding digital world.

The Fraud Hexagon provides a rich conceptual tool for understanding fraud risks in a digital business, and aims at managing fraud risks. And with findings based on the six key elements pressure, opportunity, rationalization, ego, collusion, and motive analysis organizations have an overall view of what makes fraud happen. This model offers a structure for dealing with and combating the abuse of digital platforms. Greater understanding of these interdependencies allows organizations to improve their ability to prevent, detect, and respond to new cyber threats, and contributes to the overall security posture of and trust in digital systems.

Integration of AI in Fraud Prevention Strategies

Introduction The application of artificial intelligence (AI) in building up a fraud prevention capabilities is increasingly being exploited in combating financial fraud and cybercrimes. ML and DM based AI techniques are particularly effective in recognizing and preventing fraudulent activities, because of their ability to process big data efficiently at a relatively low computation cost when compared to their traditional counterparts. This response includes a few studies on the use of AI for better fraud detection. One powerful advantage of applying AI to fraud detection is the ability to handle and analyse large amounts of data and to identify patterns that look like fraud. Sushkov et al. (2023) recognize the combined approach of the use of data mining tools including Benford's law and machine learning and propose a framework for fraud detection in the financial control process. This allows businesses to find unexpected patterns and edges cases in financial transactions, which often indicate fraud. Similarly, (Mardjono 2024) shows that, decision making and fraud detection by discovering the vulnerability of internal control in big data analytics. The ability of AI to analyse and make sense of large volumes of data, enables auditors to identify outlier items typically not identified through standard audit processes. In addition, this application of AI in fraud detection extends to developing predictive models to predict the likelihood of a fraud transaction. For instance, the study of (Nurcahyono et al., 2021)illustrates the use of predictive analytics in assessing the risk of fraudulent financial statements. Based on historical data and key risk factors, the organizational can proactively insert controls to deter fraud risks. This predictive power is supported by the findings in (Morales et al., 2022) that demonstrate the effectiveness of Benford's Law for integrity checks on large datasets showing how AI can enhance the confidence in fraud detection methods. AI is also invaluable in enhancing internal audit efficiency. The application of big data analytics

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

in audit engagement also leads to real-time monitoring and fraud detection (Rosnidah et al., 2022) which contribute into a higher audit quality (as a whole). The research shows that auditors, using software developed with AI technology, can more easily identify anomalies and red flags, allowing interventions to occur before fraud takes place. Furthermore, AI implementation in internal audit functions can substantially boost the effectiveness of prevention of fraudulent activities through promoting proactive risk management (Khikmah et al., 2023).

Beyonddetection, AI can contribute to more comprehensive fraud prevention models that span parts of an organization. (Akinbowale et al., 2023) presents a multi-objective integer programming-based optimization model to allocate anti-fraud capacity in the fight against cyber fraud, by showing how AI can be applied to the optimization of resource allocation in the design of improved fraud reduction strategies. This process underscores the importance of strategically and proactively planning for and resourcing against fraud, particularly within the complex digital environment. Finally, the moral dimensions of AI in fraud prevention are not to be neglected. As more and more enterprises and organizations turn to AI, it's increasingly important that these systems are developed and deployed with ethics in mind. The vis during auditors must incorpo rid cleared ai (Kassem, 2023) has indicated that it must reminders of servities of stress the independence, objectivity and squadoning reliability of the auditor reports as it enhances the performahes and accounting professional standards. Leveraging AI in the battle against fraud presents significant advantages in efficiency, accuracy, and the ability to manage risk in real time. With advanced data analytics and machine learning, organizations have a powerful new weapon to improve fraud detection and gain more insight and ability to spot emerging fraud. In shaping the future of fraud, AI will continue to play a critical role in helping organizations protect themselves from financial impropriety.

METHODS

Our investigation employs a Systematic Literature Review (SLR) in order to evaluate the field of cybercrime within the frame of the Fraud Hexagon. The SLR approach is selected to guarantee a systematic and disciplined survey of prior art on digital fraud studies, theories and empirical results. The review is conducted systematically, through the process of finding, selecting, assessing, and collating studies from reputable sources, including academic journals, conference and industry papers, and published findings from governments.

The research starts by articulation of concise research questions that focus on analyzing cyber fraud patterns on the light of the Fraud Hexagon framework. The literature search was based on academic papers available in the Scopus database with the key words "fraud" and "cyber" that yielded 2,201 publications. In order to guarantee that the information was up to date, the review ranged from papers published from 2019 to 2025, obtaining a total number of 887 documents. Filtering then on related subject areas such as Management and Accounting, Economics, Econometrics and Finance, the number of documents became 441. Of these, 360 were specifically related to the articles on the Fraud Hexagon framework. Based on the title and abstract, 110 papers have been selected for the study. Eligibility criteria are designed to select for high-quality and pertinent studies, and discount stale or non-peer-reviewed sources.

For robustness and trustworthiness, analysis of the literature review adopts thematic coding and qualitative synthesis. Themes such as fraud incentives, recent cybersecurity threats, and digital fraud risk prevention techniques are identified, classified, and analysed through the Fraud Hexagon model. Finally, the research examines the limitations of previous research and

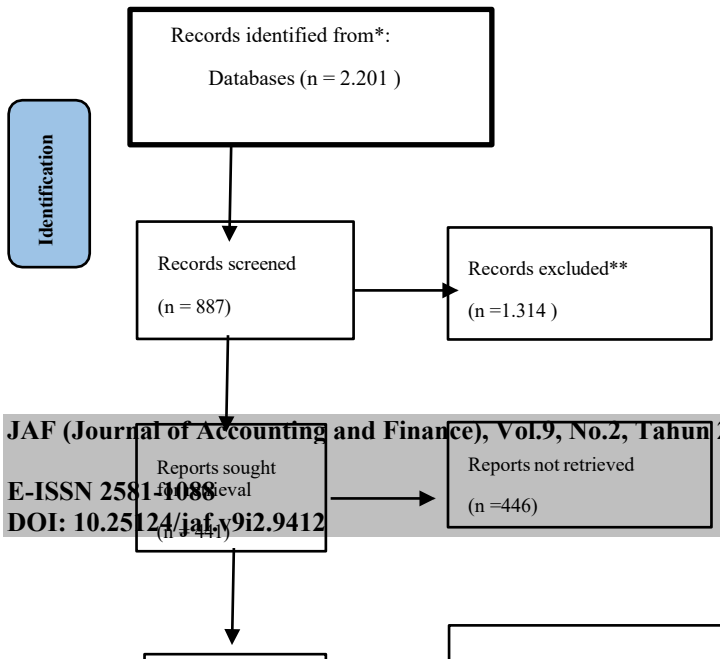
E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

how the Fraud Hexagon can be used to extend the knowledge of cybercrime beyond the traditional fraud frameworks.

Using the meticulous Systematic Literature Review methodology, this study offers a structured, thorough, and evidence-based evaluation of the bewildering landscape of digital fraud. This study systematically synthesizes and critically evaluates extant academic literature, industry reports and empirical evidence to enhance our understanding of the multi-faceted phenomenon of cybercrime and its control in an era of growing digitalization of the global economy. The SLR approach facilitates an in-depth analysis of the critical issues, patterns, and shortcomings present in the current literature, with implications for the academic debate and real-world initiatives aimed at combatting the increasingly alarming challenges of fraud in an online environment. The strong and systematic foundation of studying cybercrime based on the Fraud Hexagon model places this study as a useful resource for organization, policymakers, and practitioners to shape a comprehensive and responsive cybersecurity practices on the emerging fraud threats in the cyberspace.

Cyber Crime and Digital Fraud emerge everywhere, some countries such as USA, UK and China experience a large number of Cybercrime and Digital Fraud cases in the last years. These nations are facing the difficulties inherent to a new type of criminal activity in the digital era, criminal activity that does not fit comfortably into old fraud models. The rise in cybercrime rates in these key economies only further emphasizes the requirement for a structured and flexible response against the many guises of online crime. Amidst rapid technological progress and a proliferation of new opportunities for abuse, those countries will need to develop strong cybersecurity capabilities, regulatory approaches that are conducive to action, and close inter-border cooperation to effectively combat the increasingly powerful and extensive challenges of fraud on the digital frontier.

The thematic coding and qualitative synthesis have been carried out within the PRISMA framework. Specifically, the systematic literature review employed PRISMA to ensure a structured and transparent process for identifying, selecting, and evaluating relevant studies. During this process, themes such as fraud incentives, cybersecurity threats, and digital fraud prevention techniques were identified, classified, and analyzed using thematic coding. This approach facilitated a comprehensive synthesis of the literature, emphasizing patterns, limitations, and areas for further research within the context of cybercrime and the Fraud Hexagon model



E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

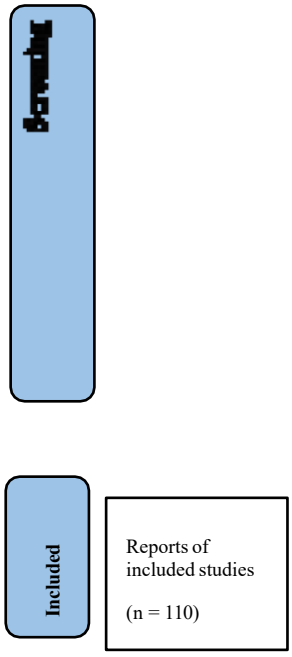


Figure 1. PRISMA Flowchart of Identification and Selected Studies

The Prisma framework, a comprehensive and widely-recognized approach for conducting systematic literature reviews, offers a structured and rigorous methodology for assessing cybercrime through the lens of the Fraud Hexagon model. This framework provides a systematic and transparent process for identifying, selecting, evaluating, and synthesizing relevant literature from a variety of credible sources, such as academic journals, industry reports, and government publications. By employing the Prisma approach, researchers can undertake a thorough examination of the key themes, trends, and gaps in the existing scholarship on digital fraud and its connection to the multifaceted Fraud Hexagon framework. This systematic and wide-ranging review process will provide an understanding of the sophisticated and dynamic character of cybercrime and of the mechanisms that facilitate and drive deceitful practices in the online era. The Prisma process's comprehensive and transparent methods guarantee that the resulting research findings are firmly rooted in empirics and can contribute both to academic discussion and effective countermeasures against increasing digital threats of fraud.

The thematic analysis process described in the document involved a systematic approach to qualitatively synthesize the literature on cybercrime within the framework of the Fraud Hexagon. The study adopted thematic coding and qualitative synthesis to identify, classify, and analyze key themes such as fraud incentives, cybersecurity threats, and digital fraud prevention techniques .The emphasis on systematic literature review methodology suggests that the process involved rigorous manual coding, thematic classification, and synthesis of findings to ensure consistency and comprehensiveness. Regarding bias mitigation in theme selection, the methodology emphasizes the structured and systematic nature of the review, which typically involves multiple stages such as independent coding, cross-verification, and consensus discussions to reduce subjective bias. Furthermore, using a literature-based thematic approach grounded in multiple sources enhances objectivity, as themes emerge from diverse empirical and

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

theoretical data rather than researcher opinion alone.

The principle investigator is directly involved in the coordination of the research (i.e. designing the study, defining the research questions, and objectives; methodology). They lead in the undertaking of systematic literature review, selection of relevant sources, thematic analysis and synthesis of findings. Furthermore, the first author also writes the manuscript to guarantee coherence as well as academic and scholarly orientation. They also manage the process of submission, response to peers' reviews, and undertake necessary revisions to improve the quality of the study. In addition, the lead author works closely with any co-authors, to facilitate efficient collaboration, and keeps everyone fully informed during the research process.

RESULT AND DISCUSSION

The following table summarizes the key findings from several sources obtained through a comprehensive search of the Scopus database. These findings provide a comprehensive overview of the current research on cybercrime and its connection to the Fraud Hexagon framework. The table below presents a detailed analysis of the various elements of the Fraud Hexagon and how they relate to the growing threat of cybercrime in the digital age.

The prominence of cited research originating from Indonesia, Malaysia, and Nigeria indicates that much of the current literature on cybercrime and the Fraud Hexagon framework is contextually rooted in these regions. While these studies provide valuable insights into the behavioral, technological, and organizational factors influencing digital fraud within these contexts, their direct generalizability to Western or broader international settings warrants careful consideration. Regional differences—such as technological infrastructure, regulatory environments, cultural attitudes toward fraud, levels of digital literacy, and the maturity of cybersecurity practices—can significantly influence the nature and prevalence of cybercrimes and the effectiveness of countermeasures . For instance, the cyber threat landscape in developing countries with emerging digital economies may differ from that in Western countries characterized by more advanced cybersecurity protocols and regulatory frameworks. However, fundamental aspects of the Fraud Hexagon, such as the core drivers of fraud—pressure, opportunity, rationalization, and ego—are theoretically universal and can be applied across diverse settings. Moreover, digital fraud techniques and cybercrime trends—such as the use of social engineering, malware, and data breaches—are often global in nature, making certain findings transferable. To enhance generalizability, future research should consider cross-cultural validation, comparative studies, and context-specific adaptations of the Fraud Hexagon framework. Incorporating empirical data from Western or international environments can help determine which aspects of the findings are universally applicable and which require localization. Therefore, while the core principles and mechanisms elucidated in the current regionally concentrated literature are valuable, their application to Western or global contexts should be done cautiously, supplemented by region-specific investigations .

Table 1
In-Depth Analysis of Contemporary Research on Cybercrime and the Fraud Hexagon Framework

Paper	Methodology	Main findings

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

Development of a multi-objectives integer programming model for allocation of anti-fraud capacities during cyberfraud mitigation (Akinbowale et al., 2023)	- Identified five key human resource capacities (organization's finance department, internal audit committee, external risk manager, accountants, and forensic accountants) to include in the MOIP model based on a literature review and qualitative data - Used a multi-objectives integer programming (MOIP) model to optimize the allocation of the five human resource capacities - Validated the MOIP model using a genetic algorithm (GA) solver to obtain the Pareto-optimal solutions - The two objective functions of the MOIP model were to minimize the total cost of the human resource capacities and maximize the forensic accounting capacities	- The MOIP model was able to find a Pareto front of optimal solutions that simultaneously minimized the total allocation cost of anti-fraud capacities and maximized the forensic accounting capacities in cyberfraud prone areas. - The MOIP model was able to find feasible solutions that achieved the stated objectives or found a trade-off between them when they could not be reached simultaneously. - The Pareto front solutions showed the feasibility of the MOIP model to achieve the objectives without violating the stated constraints.
A Comparison of Online Fraud Prevention Disclosure in Malaysian and Indonesian Public Universities (Joseph et al., 2021)	The methodology used a content analysis approach to examine the extent of fraud prevention information disclosure on the websites of Malaysian and Indonesian public universities. The researchers used a 100-item Fraud Prevention Disclosure Index (FPDi) across 8 aspects, coding each item as 1 for disclosure or 0 for no disclosure. Data was collected from the university websites over a 1-month period in 2019.	- The level of fraud prevention disclosure on the websites of Malaysian and Indonesian public universities was generally low, with Malaysian universities disclosing slightly more on average than their Indonesian counterparts. - Malaysian universities were stronger in disclosing information related to internal audit and bursary, while Indonesian universities had higher disclosure in areas like integrity, governance, policy, fraud prevention strategies, and fraud response procedures. - The study found no significant differences between the two countries in the disclosure of core values, fraud prevention strategies, fraud response procedure, and raising awareness, all of which were poorly disclosed on the websites.

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

"Does forensic audit influence fraud control? Evidence from Nigerian deposit money banks" (Adesina et al., 2020)	- The study used a survey research design to collect data from the target population of bankers in Nigeria. - The population consisted of 22 deposit money banks (DMBs) operating in Nigeria, with a focus on 17 banks with international and national authorization. - The researchers distributed 200 questionnaires to the 17 selected banks and received 193 completed questionnaires, representing a 96.5% response rate. - The researchers ensured the validity of the questionnaire by pilot-testing it, getting feedback from experts, and modifying the instrument before distributing it to the target population.	- Forensic audit has a significant effect on the control of financial frauds in Deposit Money Banks (DMBs) in Nigeria. - The forensic auditor's skills and knowledge have a significant effect on the timely adjudication of financial fraud cases in DMBs in Nigeria. - The experience of a forensic auditor has a significant effect on fraud control in DMBs in Nigeria, with more experienced auditors having a stronger effect.
UNDERSTANDING ACCOUNTING FRAUD MOTIVATION, PROTECTION PROCEDURES, AND FIRMS' PERFORMANCE : EXTERNAL AUDITORS' PERSPECTIVE (Yaqoub et al., 2023)	The study used a qualitative research approach, collecting data through semi-structured interviews with seven experienced external public auditors, and analyzing the data using content analysis.	- Personal and environmental factors are the most critical accounting fraud motivations. - Examining and checking the internal audit system's strengths and weaknesses is more important in detecting fraud than training and auditing procedures. - Recovery and follow-up procedures are the most significant measures to correct fraud activities.
AUDITOR'S SKEPTICISM, FORENSIC ACCOUNTING, INVESTIGATION AUDIT AND FRAUD DISCLOSURE OF CORRUPTION CASES (Laupe et al., 2022)	- Survey methodology using questionnaires distributed to auditors at various government agencies across Indonesia - Final sample size of 118 completed questionnaires - Data analysis using structural equation modeling (SEM) with the WarpPLS 7.0 software, including model evaluation and hypothesis testing	- Forensic accounting has a negative effect on the disclosure of fraud in corruption cases. - Investigative audits have a negative effect on the disclosure of fraud in corruption cases. - Auditor skepticism can strengthen the negative influence of forensic accounting and investigative audits on the disclosure of fraud in corruption cases.

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

Predicting Risk of and Motives behind Fraud in Financial Statements of Jordanian Industrial Firms Using Hexagon Theory (Bader et al., 2024)	- The study sample consisted of listed and non-listed industrial companies on the Amman Stock Exchange (ASE) from 2012-2017. - The data was analyzed using logistic regression modeling in SPSS. - The study used a cross-sectional approach.	- An increase in ROA (a pressure motive) is associated with an increased likelihood of fraudulent financial statements. - A higher percentage of independent members in audit committees (an opportunity motive) is associated with a decreased likelihood of fraudulent financial statements. - The presence of tone-related party transactions (a collusion motive) is associated with an increased likelihood of fraudulent financial statements.
THE INFLUENCE OF FRAUD TRIANGLE FACTORS ON REAL EARNINGS MANAGEMENT (Hasnan et al., 2022)	- Sample: 557 Malaysian public listed companies (PLCs) from 2017 to 2019, resulting in 1,671 firm-year observations - Data sources: Secondary data from annual reports and financial databases - Analysis method: Multiple linear regression analysis using SPSS	- Firms with poorer financial performance, as measured by lower return on assets (ROA), are more likely to engage in real earnings management. - Firms audited by Big 4 auditors are more likely to engage in real earnings management, suggesting that Big 4 auditors are not effective at preventing such practices.
Integrating Data Mining Techniques for Fraud Detection in Financial Control Processes (Sushkov et al., 2023)	1. Conducting Benford's Law tests (basic, advanced, and associated) on the financial data to identify statistical features that deviate from the expected patterns. 2. Applying clustering algorithms to the statistical features obtained from the Benford's Law tests to identify suspicious transactions. 3. Analyzing the resulting clusters to extract insights and identify a subset of high-risk transactions that require manual examination by financial control specialists.	- The paper proposes a methodology that combines Benford's Law and clustering techniques to enhance fraud detection in financial control processes. - The application of this integrated approach successfully identified a small subset (3.61%) of suspicious transactions that warranted further investigation. - The proposed methodology is more efficient and targeted compared to manual auditing of all transactions, allowing financial control professionals to focus their efforts on the most suspicious activities.

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

Detecting Fraudulent Financial Reporting Using the Fraud Hexagon Model: Evidence from the Banking Sector in Indonesia (Achmad, Ghozali, Rahardian, et al., 2022)	- Purposive sampling of banking companies listed on the Indonesia Stock Exchange (IDX) from 2017- 2021 that met certain criteria - Quantitative analysis using logistic regression with SPSS software - Dependent variable was a dummy variable coded as 0 or 1 to indicate the presence or absence of fraudulent financial reporting - Independent variables included financial target, financial stability, external pressure, ineffective monitoring, auditor switching, change in director, arrogance, and collusion	- External pressure and arrogance affect fraudulent financial reporting in the banking sector in Indonesia. - Financial targets, financial stability, ineffective monitoring, auditor switching, change in director, and collusion do not affect fraudulent financial reporting. - Companies should focus on implementing effective human resource policies and procedures to prevent fraudulent financial reporting.
UNDERSTANDING ACCOUNTING FRAUD MOTIVATION, PROTECTION PROCEDURES, AND FIRMS' PERFORMANCE : EXTERNAL AUDITORS' PERSPECTIVE (Yaqoub et al., 2023)	The study used a qualitative research approach, collecting data through semi-structured interviews with seven experienced external public auditors, and analyzing the data using content analysis.	- Personal and environmental factors are the most critical accounting fraud motivations. - Examining and checking the internal audit system's strengths and weaknesses is more important in detecting fraud than training and auditing procedures. - Recovery and follow-up procedures are the most significant measures to correct fraud activities.

Enhancing Cybercrime Understanding Through the Fraud Hexagon Framework

Digital fraud and cybercrime have become increasingly prevalent in today's interconnected world, driven by rapid technological advancements and the growing reliance on digital platforms. As businesses increasingly digitalize their operations, awareness of the changing nature of cybercrime is critical to reducing financial losses and reputational harm. The model consists of six components to evaluate these trends in and motivational conditions of the fraudulent behaviors: pressure, opportunity, rationalization, ego, capability and collusion; this fraud hexagon has been designed to be useful in managers‟ daily activities.

One of the biggest contributors to digital fraud is financial pressure – which may lead some individuals to make poor decisions. Suryandari et al., 2023) sugests that employee in high stress work situation, such as financial institutions, are more likely to engage in fraudulent activities to cope up with economic problems. Furthermore, the liquidity stress caused by the COVID-19 pandemic resulted in fraud cases that skyrocketed (De La Torre Lascano & Quiroz Peña, 2023). This pattern endorses the criticality of understanding the economic bases of fraudulent behavior and deploying prophylactic measures in companies.

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

Digital transformation has had a slew of implications and has also left the door open for cybercriminals to capitalize on the system weaknesses. As reported by (Akinbowale et al., 2023), the availability of online mediass as defe_Soure systems, unauthorized acquisition to the confidential information has increased, and cybercriminals have the simple access to deceit. During the pandemic with the increased use of remote working and digital transactions, the avenues of exposure have grown, in some cases faster than the capacity for implementing appropriate security measures (De La Torre Lascano & Quiroz Peña, 2023). To combat these risks, businesses need to spend on strong cybersecurity defences and constantly maintain their security settings.

Another element of fraud is rationalization, which helps people rationalize their actions. The veil of anonymity that accompanies online activities is a weapon making it convenient to shrug off the moral responsibility that should come with their actions. (Damayanti & Agustia, 2024) argue that the organisational culture and individuals' own belief significantly influence how participants rationalise unethical behaviour. Therefore, creating a corporate culture that values ethics and accountability is key to reducing fraud.

Apart from motivation and opportunity, the ability of cyber criminals strongly determines the outcomes of cybercrimes. Many fraudsters have advanced technical knowledge that enables them to take advantage of security loopholes (Morales et al., 2022). As the nature of cyber threats evolves, the only way companies will be able to defend themselves is by investing in cyber security training, threat intelligence, and advanced security technology to keep the attackers at bay.

Another is collusion and joint fraud in which a group of people collaborate to scam electronic systems. According to research, fraud collusion is more challenging to identify and mitigate because fraudsters can perform elaborate techniques to prevent security measures (Suryandari et al., 2023). "If collusion rears its head, strong internal controls, greater transparency and a whistleblowing mechanism can reduce the chances of collusion," he said.

The era of big data and data analytics has changed the landscape of fraud detection and prevention. Rosnidah et al. claim that enterprises using big data analytics can now identify patterns and the way fraud operates in real time, significantly enhancing their fraud detection capabilities. It allows companies to monitor transactions in real-time, identify suspicious activity and stay ahead in the world of cybercrime through machine learning and AI-driven analytics.

About the Fraud Hexagon The Fraud Hexagon is a framework for identifying and addressing digital fraud and cybercrime. In this context, economic pressure, digital vulnerability, rationalization, technical capability and collusion, will help to assist fight to develop corporate strategies to protect and safeguard in the digital business environment.

The Fraud Hexagon offers readers a valuable tool for investigating the motivations and modus operandi of cybercrime in the digital era. The model encompasses six key elements: pressure, opportunity, rationalization, ego, ability, and collusion. With these six factors, the model provides a comprehensive 360-degree view of fraud. This paper discusses how the Fraud Hexagon framework may add to our understanding of cybercrime through a literature review of relevant works.

One important feature of the Fraud Hexagon is that it may have a meaningful comprehensive picture regarding the source behind these cyber-criminals. (Suryandarietal.,2023) indicate that individuals who are involved in fraudulent acts often rationalize their behaviors in

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

terms of pressure and context. This psychological factor playsacrucialroleinunethicaldecision-making,influencingindividualstojustifyfraudulentbehavior. Furthermore, ego is added to the framework to highlight how entitlement or superiority can also enhance fraudulence.

The identification of opportunities to commit fraud is also an important part of cybercrime. (Akinbowale et al., 2023) observe that many opportunities exist for scammers to take advantage of system weaknesses provided by Designing Hybrid-Cloud Systems 229 the digital terrain. Online anonymity makes it harder for them to be tracked down, thus giving cybercriminals a more free hand. Identifying these opportunities helps the organization mount more effective defenses against possible attack.

Collusion is yet another vital aspect of cyber fraud. Cyber-criminals often work together and plan sophisticated frauds, complicating its detection and prevention. Collusion-Resistant Strategy According to (Suryandari et al., 2023), fraud schemes are likely to be more successful if they are performed by several actors and businesses should elaborate anti-collusion strategies. The potential and expertise of criminals also define the type of digital fraud. (Morales et al., 2022) highlight that many cybercriminals have high technical skills and are able to effectively take advantage of weaknesses in systems. With cyber threats becoming more advanced, businesses need to regularly update their equipment and protocols to fight account fraud.

Apart from this, the Fraud Hexagon structure also has practical implications in preventing fraud. Auditors can utilize this framework to perform fraud risk assessments based on a variety of complex pieces of evidence. (Kassem, 2023)"and how auditors can use the structure approach to identify fraud risks more thoroughly, as well as design good internal control to minimize threats.

Thirdly, the Fraud Hexagon gains new importance in the digital era for comprehending cybercrime. The spread of digital transactions, particularly during the COVID-19 pandemic, has opened the doors to new fraud opportunities. (De La Torre Lascano & Quiroz Peña, 2023) state that organizations should implement a broad fraud-prevention program that includes the risks of cyberfraud. By incorporating the Fraud Hexagon into standard cybersecurity frameworks, businesses as well as policymakers will be able to design more agile and situationally aware fraud risk prevention schemes in an ever-digitalized world.

Common Types of Digital Fraud and Their Alignment with the Fraud Hexagon

Fraud in the digital world takes many faces, all in line with the facets of the Fraud Hexagon model – pressure, opportunity, rationalization, ego, capability and collusion. Delineating these typologies of digital fraud with the concept of these attitudes can assist organizations in devising more successful prevention and detection methods. One of the most widespread types of digital crime is phishing, when bad actors mimic an authentic party to trick you into giving them sensitive information like a password or a credit card number. This fraud type reflects the opportunity dimension of the Fraud Hexagon because the internet is a large and open market allowing fraudsters access to potential targets. Without minimizing the role of the pressure element; employees may be expedite or feel pressured to respond to the urgencies of the trusted party, causing people to make quick and harmful decisions that impaired them to secure (Suryandari et al., 2023).

Identity theft is another prevalent fraud scheme in which an individual's personal information is used to perpetrate fraud (e.g. open credit accounts, make purchases) without his or her consent. This type of fraud is particularly related to expertise, as it needs certain technical

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

knowledge to get and use personal information which ia a form of fraud. Rationalization is also relevant in this context, as offenders may rationalize their behavior as no direct harm is being done to the victim or consider they have a right to exploit the information for personal benefits (Parluhutan et al, 2022). Likewise, credit card fraud is when someone illicitly takes another's credit card information and purchases items with it. This scam is particularly driven by the opportunity factor, as online shopping has made it more convenient to exploit weaknesses within payment mechanisms. The pressure element can be observed too as there may be financial desperation among the people and they do not report small fraudulent activities, thereby enabling the fraud to thrive with such impunity (Akinbowale et al., 2023).

Business Email Compromise (BEC) is another advanced fraud, where fraudsters pretend to be executives or reputable partners and dupe employees into sending funds or confidential data. This scam category fits the Fraud Hexagon's collusion characteristic, as these operations frequently require several individuals to pull it off. The ego component plays a part, since people may feel important or compelled to respond to email from high-status individuals, which leads to lower-quality decisions (Abdullah et al., 2022). On the more offensive end of the spectrum of cybercrime, ransomware attacks are carried out through malware that locks up a victim's data and then demands payment to return control of it. Such a fraud shows the skills dimension, the attacker need to be skillful in order to implement the attacking effectively. The pressure dimension is relevant, because organizations might feel pushed to pay ransoms faster, to recover their essential data and may not completely think over the risks (Martins & Júnior, 2020).

Furthermore, fraud from online auction and marketplace sellers, who send nothing if they've even sent anything at all after you've paid for it, happens. This type of crime is consistent with the rationalization component, since those committing fraud may rationalize that they are not really committing a "crime" or that their victims have enough money to handle the loss. The factor of opportunity is also essential, since the anonymity of online payments can facilitate criminal behavior (Sánchez Henríquez et al., 2022).

The use of the Fraud Hexagon is crucial in pinpointing cyber fraud, as this organizes different motives and methods of committing cyber crime. Studying the six components of the Fraud Hexagon –pressure, opportunity, rationalization, ego, capability, and collusion–can help companies create better strategies to detect or prevent fraud. Pressure is a great motivator, especially in high pressure situations such as financial instability and unrealistic performance expectations that ultimately push people into fraud. For instance, (Suryandari et al., 2023) reveal the effect of economic stress on employees rationalizing towards the fraud. Opportunity is also relevant, since digital platforms can be exploited in various ways. Akinbowale et al. (2023) argue that unauthorized access to sensitive content provides an opportunity for fraud that entails attackers to strengthen cyber security measures such as multi-factor authentication and regular security audits. Justification also affects misconduct, when people persuade themselves that the ends justify the means. (Damayanti & Agustia, 2024) highlights that personal beliefs and organizational culture have a significant role in developing these rationalizations and the necessity of cultivating an ethical understanding was also underlined. The ego aspect relates to the fraudsters confidence level and sense of self, and the belief in the safety of cyber space. This attitude may be addressed through promoting ethical responsibility and whistle blowing. Another important aspect is capability as cyber criminals are technical savvy and take advantage of system vulnerability. (Morales et al., 2022) highlight the need for cybersecurity training to help control fraud within an organization. By focusing on these six areas, companies can mitigate the risk of cyber fraud and avoid the significant financial and reputational damage it can have on an organization.

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

The wide spread of digital fraud highlights the vital necessity to understand the motivations and conditioned patterns of behaviour anarchistic perpetrators among cyber-criminals using Fraud Hexagon structure. By understanding and dealing with the interconnected elements of pressure, opportunity, rationalization, ego, capacity and collusion that support these schemes, organizations can put in place more comprehensive fraud prevention and detection programs. This multi-faceted approach is absolutely essential to staying ahead of the constantly changing and more sophisticated environment that is digital fraud and cybercrime.

Key Challenges in Detecting and Preventing Cyber Fraud: Perspectives for Individuals and Organizations

With the cyber age, identifying and stopping cyber fraud has been a difficult task for individuals and businesses. The more sophisticated cyber frauds become, the more risk they spawn, which is why preventing fraud also requires a multi-layered strategy. This is an aggregate response to the perspectives presented on the primary challenges in controlling cyber fraud through literature. One of the biggest problems with cyber fraud is how the methods used by fraudsters constantly change. As emphasized by Suryandari, the underlying reasons for engaging in fraudulent conduct can be explained by the Fraud Hexagon Theory which suggests incentives, opportunity, rationalization, and MD-like characteristics as the main drivers for fraud (Suryandari et al., 2023). This model highlights the importance for companies to consider psychological and situational aspects that can predispose an individual towards committing fraud.

It also reflects the importance of knowledge of the motives for accounting fraud in the development of prevention methods (Yaqoub et al., 2023). A second, equally important challenge is that of using a traditional auditing approach, which may not be enough in confronting the advanced global cyber fraud attacks. Although Benford's Law can be a useful integrity testing tool, the effectiveness of this test may differ depending on the module, which suggests that a one size fits all approach may not be appropriate for all contexts (Morales et al., 2022) This implies that organizations need to upgrade their fraud detecting capabilities by using advanced data analytics and forensic accounting techniques. Akinbowale et al.(2023) developed a multi-objective framework for anti-fraud resource allocation in which anti-275 fraud allocation can help an organization to optimize the target of their mitigation strategies (Akinbowale et al., 2023). In addition, the efficacy of internal controls and audit committees greatly aids the war against cyber fraud. Handayani and Kawedar also discovered that frauds can be limited from occurring by implementing strong internal controls to minimize susceptible points (Handayani & Kawedar, 2021). In addition, the existence of an effective audit committee has a moderating role in mitigating the fraudulent financial reporting as in the mining sector in Indonesia (Sari et al., 2022). This is obviously an excellent way of promoting anti-general fraud by rule. Awareness and training are also major factors in the fight against cyber fraud. Findings of Kassem's study suggest that the effect of fraud characteristic's on the auditors' FFR risk assessment is of primary importance, and reflects the importance of having trained and educated auditors on fraud detection (Kassem, 2023). Furthermore, Alrawashedh results show that organizations have to foster a culture of accountability and transparency to improve their fraud detection endeavors (Alrawashedh, 2023).

Cyber-attacks and cyber fraud as a whole are increasingly challenging to detect and prevent whether at individual or corporate level, since fraudsters take advantage of weaknesses in cyber resources. These obstacles can be analyzed in the framework of the Fraud Hexagon, which explores the dimensions of pressure, opportunity, rationalization, ego, capability, and collusion in the perpetration of fraud. There are of course pressures, as financial pressure, pressure to perform,

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

pressures which lead people to behave in unethical ways. (Suryandari et al., 2023) emphasise that financial distress frequently motivates employees to perpetrate fraud in order to fulfill financial commitments or work goals. Organizations should recognize these pressures and develop a culture of support to help reduce the risk of fraud. Opportunity also enables cyber crime, as there are many opportunities for victimization using online facilities. (Akinbowale et al., 2023) emphasise that unauthorised access to information, especially sensitive ones, is of a high concern as adoption of digital technology has accelerated after the pandemic (De La Torre Lascano & Quiroz Peña, 2023). These weaknesses need to be addressed with strong cybersecurity approaches and risk assessments. Re\-ationalization Displacement Facilitates offenders to justify their action, minimizing consequences or consider themselves as having the right to acquire fraudulent proceeds (Damayanti & Agustia 2024). Fostering ethical conduct and responsibility in organizations might reduce this tendency. Ego is a factor in cyber deception as well, as we know that criminals believe they can get away with such activities because they think that they are anonymous in the digital realm.

This overconfidence can be countered by fostering a culture that emphasizes ethical responsibility and vigilance. They are also a critical because cybercriminals use their advanced technical capabilities to take advantage of system weaknesses. Morales et al. (2022) highlight the need for ongoing training and strong investment in cybersecurity to keep up with a dynamic threat landscape. Collusion introduces more fraud risk, as the type of digital connection means that people can easily work together to create and implement fraudulent schemes. According to (Suryandari et al., 2023), organizations should focus on transparency provisions by conducting regular audits, and setting a whistleblower policy, in order to prevent collusion. By leveraging these challenges via the F/the Fraud Hexagon model, a more effective approach to detect and prevent cyber fraud can be constructed.

Benefits and risks AI-supported fraud prevention approaches have their specific pros and cons which companies should be aware of to optimally leverage these technologies. Using the Fraud Hexagon model – pressure, opportunity, rationalization, ego, capability and collusion – businesses can consider how AI boosts fraud detection and also identify its limitations. One including most characteristic forces of AI for fraud protection is the improvement in detection capacity. Learning machine algorithms can process huge volumes of data on the fly to uncover patterns and irregularities that may signal fraudulent activity. (Sushkov et al., 2023) also researches the integration of data mining methods, including Benford's Law, for enhanced fraud detection accuracy. In addition, AI makes repetitive tasks automated so that auditors can concentrate on more sophisticated fraud detection activities. (Nonnenmacher & Gómez, 2021) highlight the value of unsupervised anomaly detection methodologies in internal audit, through the lenses of reengineering and human workload reduction. There's also the benefit of prediction, wherein AI can forecast potential fraud risks by analysing historical premonitory data. (Morales et al., 2022)analyze how AI increases applicability of integrity tests on large database logs by providing early anomaly identification. Similarly, AI enhances the risk assessment by considering economic pressures and organizational weaknesses, which help distribute anti-fraud resources better (Akinbowale et al., 2023).

However, AI-driven fraud prevention also has limitations. One of the most demanding tasks is on data quality; incorrect data or incomplete data would result in low accuracy of fraud detection, this shows the importance of data stewardship. It is additionally hard to implement, and the implementation can be expensive, since it can be difficult to incorporate AI tools into an

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

organization's current system and often takes training in uniquely talented staffs to succeed at maintaining these methods. A further limitation is its susceptibility to false positives (i.e., correctly denied) if transactions of legitimate merchants are incorrectly marked as fraudulent, which causes futile potential business interruptions. There are also ethical and legal considerations that make the adoption of AI even more interesting, in the sense that the use of the individual's personal information to detect fraud has posed privacy issues and regulatory challenges. AI-powered fraud detection should not infringe upon privacy laws to protect organizations from potential litigation and damaging their reputation. Finally, fraudsters' tactics change which creates an ongoing challenge, when the fraudsters adapt to avoid AI detection. (Damayanti & Agustia, 2024) emphasizes the changing nature of rationalization in criminal behavior and the need to continuously update and improve our AI systems. AI Fraud Prevention offers enormous advantages from the perspective of fraud detection and prevention, however, the following challenges must be confronted in order to carry out its implementation effectively and ethically.

Effectiveness of Current Cybersecurity Measures in Preventing Digital Fraud

Preventing fraud The issue of prevention in a digital, cyber securitized age has never been more critical for organizations across all sectors. The adoption of modern technologies (e.g., big data analytics, forensic accounting) has greatly increased the ability of companies to identify and prevent fraud. Nevertheless, the increase of fraud methods requires constant enhancement of such countermeasures. Big data analytics (BDA) One of the breakthroughs related with the fraud detection is adoption of the big data analytics. BDA has the capability to sift through enormous amounts of data to detect trends and irregular patterns that may lead to fraudulent activity. For example, Mardjono (et al, 2024) clearly contends that BDA and data-mining applications provide the audit institutions with better decision-making and fraud detection. Furthermore, combing data mining methods with traditional audit procedures has also been adopted in financial control processes for improving the detection of fraudulent activities, such as (Sushkov et al., 2023) presents a framework incorporating Benford's Law and machine learning algorithms to strengthen fraud detection. In addition, the importance of internal controls and audit committees cannot be overemphasized. In order to make fraud less likely, good internal control is needed, in accordance to Handayani and Kawedar who discover that it has been proven that the existence of strong internal control systems can reduce the opportunity of fraud (Handayani & Kawedar, 2021). Furthermore, the existence of an effective audit committee has a moderating effect in diminishing fraudulent financial reporting (as show in research conducted in the Indonesian mining sector (Sari et al., 2022). This underscores why it is so important to have good governance in place to supplement anti-fraud efforts." Forensic accounting methods also contribute significantly to the field of fraud prevention and detection. These procedures help auditors perform detailed inquiries on financial variances and aspects that it should improve the audit's quality. For example, the research of Adesina et al. underscores the need for banks to create specialized forensic units for aevery-day fraud fighting (Adesina et al.

In addition, the results of Kassem show that the auditors' attitudes to factors related to fraud have an impact on their evaluation of risks of fraudulent financial reporting.The awareness and training programs in the area of fraud can contribute to the improvement of the audit quality. Despite these advancements, challenges remain. Fraud has taken on a nimble approach, so companies need to stay on their toes. For instance, the findings of Yaqoub indicate that while IT can reduce the risks for fraud, monitoring the capabilities of internal audit system in order to effectively detect any fraud must be attentive to their strengths and weakness (Yaqoub et al., 2023). Moreover, the results of Morales et al. show that despite Benford's Law being an effective tool for integrity tests, it may not always result in similar behaviour across various modules

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

indicating that fraud detection requires a more sophisticated approach (Morales et al., 2022).

Some studies examined audit rules and frameworks for fraud detection and prevention. Advanced methods like data mining and forensic accounting may help organizations uncover fraud. For instance, (Sushkov et al., 2023) emphasize the relevance of data mining and Benford's Law in automating and expanding financial control fraud detection, improving audit efficiency. Similarly, Rosnidah et al. highlight auditors' use of Big Data analytics to detect and prevent fraud and the pros and cons of incorporating it into audit (Rosnidah et al., 2022). Audit quality and fraud detection depend on auditor ethics and incentives. According to Parluhutan et al. (2022), auditor motivation, ethics, and professional skepticism affect audit quality. A motivated auditor is more likely to have integrity and accurate audit results. C Damayanti (2024) proving that personal and organizational values affect auditor performance. Regulation and Fraud Rates Regulatory environment and governance frameworks affect prevention, detection, and remedy. Governance measures may increase financial responsibility and reduce LG fraud, according to Din et al. (2022). Kassem (2023) also indicates that top management integrity is important for fraud risk assessment and that a strong ethical culture may prevent fraud leakage. According to Morales et al., employing Benford's Law in audit truth tests emphasizes the need for effective governance to sustain financial trust (Morales et al., 2022). Internal audits and strong internal control systems are crucial to fraud prevention. Khikmah et al. (2023) argue that transformational leadership and internal audit processes can prevent fraud and that organisation leadership should ensure that work environments do not encourage fraud. Nurcahyono et al. (2021) also argue that effective whistleblower mechanisms and active audit committees reduce fraud by demonstrating that internal controls prevent fraud.

Strategies for Strengthening Fraud Prevention and Detection Using the Fraud Hexagon

To properly deal with these problems, companies need to utilize a multi-faceted approach that includes improving internal controls, promoting ethics, training personnel, and using technology to find fraud. Fraud Hexagon has six parts: pressure, opportunity, rationalization, ego, collusion, and financial stability. These are all things that might cause fraud to happen in a company (Bader et al., 2024; Suryandari et al., 2023). Companies may make a plan to lower the risk of these variables once they know what they are. Internal controls are especially important since they directly address the risk of fraud. Studies demonstrate that good internal controls may make it far less likely for fraud to happen by making sure that different parts of the organization keep an eye on each other (Ait Novatiani et al., 2022; Alrawashedh, 2023; Putra et al., 2022). A good internal audit function and risk management, for example, may help reduce false financial reporting (Ait Novatiani et al., 2022).

An ACC may also act as a moderation variable, and this impact makes the internal controls perform better to stop fraud (Mousavi et al., 2022; Sari et al., 2022). Creating an ethical climate in the workplace is just as important. A strong ethical culture may help workers deal with the stress and reasons they might have to act dishonestly. Companies that care about doing the right thing and running their businesses well are less likely to be victims of fraud, according to studies (Martins & Júnior, 2020; Yami & Poletti-Hughes, 2022). Training classes on ethical behavior and showing workers the effects of fraud may help strengthen this commitment and make employees more accountable (Jamieson et al., 2019). Training certain employees is very important for them to learn about and comprehend different ways to find fraud. Training programs that teach workers how to spot and stop fraud might turn them into watchful watchdogs inside the company

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

(Jamieson et al., 2019; Yaqoub et al., 2023). Also, teaching workers about the Fraud Hexagon could provide them a rudimentary idea of what fraud is and how they can help stop it (Jamieson et al., 2019). This kind of proactive strategy not only makes it easier for an organization to find fraud, but it also fosters a culture of openness and honesty. In this digital era, it's more crucial than ever to employ technology to stop fraud. More sophisticated data analytics and machine learning techniques may be utilized to find unusual behavior and patterns that indicate fraud (Mardjono et al., 2024; Rosnidah et al., 2022; Sushkov et al., 2023). For example, using data mining techniques with standard auditing methods may help find more financial crimes and make fraud detection methods more effective (Mardjono, Jooban, Abdullah, and Away, 2024; Sushkov, Suvorov, and Barakhnin, 2023). Also, you may use technologies like Benford's Law to look for fraud in huge data and many more to make the protector stronger against financial crimes (Morales et al., 2022; Sushkov et al., 2023).

Combating the issues of fraud within organizations must take on a holistic approach, with consideration of the consequences of the Fraud Hexagon. This theoretical model helps to understand the dynamics of the elements that support a culture of fraud -such as pressure, opportunity, rationalization, ego, collusion and financial stability (Suryandari et al, 2023)- and in maneuvering such challenges; organizations need to take into consideration their future consequences to organizational integrity and stakeholder trust. What are people looking for?.k Pressure-accounting employees are under that they excuse their financial irregularities. According to studies, high pressure at the organization level, particularly of financial performance, can greatly lead to the occurrence of fraud (Khatib et al., 2022). For example, an auditor with a high queasiness level to retain the job may avoid finding distortion to one’s organization expectation (Damayanti, 2024). To address this, an organization should create a climate that encourages openness and honesty that could counterbalance the pressures sustaining fraud (Alrawashedh, 2023). Such change in culture is possible by establishing strong internal controls and ensuring that accountability standards are present at all echelons in the institution (Alrawashedh, 2023). A second major challenge is the potential for fraud resulting from weak internal controls and monitoring. Research has confirmed that firms with poor internal control are more vulnerable to fraud (Morales et al., 2022).

The importance of implementing forensic accounting techniques as a tool to improve fraud detection capacity was underscored (see Dworkin, 2023). By attaching forensic accounting as part of corporate governance, an entity not only will have the ability to detect fraud more efficiently ontime, but also future the fraud to occurred, caused the environment of more control to the work misconduct. In addition, the use of innovative data analytics and machine learning solutions can significantly improve the detection of anomalies in financial transactions, potentially making fraud detection more effective (Sushkov et al., 2023). The future stakes for such challenges are enormous. Organisations who are increasingly using technology to detect fraud should also be mindful that cyber fraud in particular has been exacerbated by the increase in digital transactions (Jamieson et al., 2019). This requires ongoing technology investments in technology and training, to ensure staff are able to detect and address tonight's fraud risks (Mardjono et al.,2024). Furthermore, the changing regulation of corporate governance and fraudulent practices will cause companies to change their practices to meet compliance standards and retain the trust of stakeholders (Martins & Júnior, 2020).

CONCLUSION, LIMITATION, AND SUGGESTION

Overall, dealing with issues of fraud is a multifaceted challenge of how to think about and manage such behavior in organizations. This includes building a comprehensive ethical culture

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

that values ethics in all that we do, from honesty and transparency to accountability. It also includes the adoption of strong internal control like effective scope of internal audit, risk Management System, audit committee which could provide an effective system of check and balances that mitigate the risk of fraud.

In addition, you must invest in thorough employee training programs. Such programs should emphasize fraud prevention and detection skills, enabling staff members to serve as watchful stewards, and help them to identify the red flags of fraud. Providing employees with information on the Fraud Hexagon model can help them learn about the different elements of fraudulent behavior and their part in reducing these risks.

The use of cutting-edge technologies to detect fraud, such as data analytics and machine learning, will yield significant improvement in a company's ability to detect anomalies and detect patterns in fraudulent behaviour. The use of these new tools combined with traditional audit methods can greatly enhance a business's fraud prevention systems. With attention to the Fraud Hexagon framework, and taking a comprehensive approach, organization can improve their fraud prevention, detection, and response capabilities. This will, in at least some cases, safeguard them against the risk of losing credibility with their stakeholders.

A number of promising directions for further research in this field exist with the potential to improve the prevention and detection of fraud. Organizational culture and leadership as determinant factor of the articulate of ethics and fraud prevention takes a mediatory role. This also includes examining how corporate values, management techniques and leadership role-modeling affect the behavior of employees and the vulnerability of an organization to fraud. Future studies may consider the extent to which organization specific employee training programs influence employees/organizations to detect and prevent fraud. An evaluation of initiatives involving fraud awareness and detection techniques and even creating a vigilant, integrity-based faculty would be invaluable.

The real life implementation of advanced data analytics and machine learning in the area of financial fraud detection is a further challenging research line to pursue. It involves scrutinising the truthfulness, effectiveness and productivity of these technologies when it comes to detecting anomalies and extracting fraudulent patterns. Moreover, it is important to study the new threats and vulnerabilities that are raised and associated with this upward trend in cybercrime and digital transactions. Further research is needed on digital systems vulnerabilities, cybercriminal tactics and on benchmark models that could help defend organizations and stakeholders in the future.

Future research might explore the impact of regulatory changes and evolving corporate governance norms on efforts to prevent fraud. By measuring the impact these laws have on ethical behavior, internal controls and transparency organizations can become more effective in their compliance programs and can better prevent financial misconduct.

REFERENCES

Abdullah, M. I., Sudirman, Masdar, R., Din, M., & Firman, M. F. (2022). ANTECEDENTS OF THE ACCOUNTABILITY IN INDONESIAN LOCAL GOVERNMENT FINANCIAL REPORTING.
International Journal of Professional Business Review, *7*(5).
https://doi.org/10.26668/businessreview/2022.v7i5.e709

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

Achmad, T., Ghozali, I., & Pamungkas, I. D. (2022). Hexagon Fraud: Detection of Fraudulent Financial Reporting in State-Owned Enterprises Indonesia. *Economies*, *10*(1). https://doi.org/10.3390/economies10010013

Achmad, T., Ghozali, I., Rahardian, M., Helmina, A., Hapsari, D. I., & Pamungkas, I. D. (2022). *Detecting Fraudulent Financial Reporting Using the Fraud Hexagon Model: Evidence from the Banking Sector in Indonesia*. https://doi.org/10.3390/economies

Adesina, K., Erin, O., Ajetunmobi, O., Ilogho, S., & Asiriuwa, O. (2020). Does forensic audit influence fraud control? evidence from Nigerian deposit money banks. *Banks and Bank Systems*, *15*(2), 214–229. https://doi.org/10.21511/bbs.15(2).2020.19

Ait Novatiani, R., Afiah, N. N., & Sumantri, R. (2022). RISK MANAGEMENT AND OTHER FACTORS PREVENTING FRAUDULENT FINANCIAL REPORTING BY STATE-OWNED ENTERPRISES IN INDONESIA. *Asian Economic and Financial Review*, *12*(8), 686–711. https://doi.org/10.55493/5002.v12i8.4587

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2023). Development of a multi-objectives integer programming model for allocation of anti-fraud capacities during cyberfraud mitigation. *Journal of Financial Crime*, *30*(6), 1720–1735. https://doi.org/10.1108/JFC-10-2022-0245

Alrawashedh, N. H. (2023). Factors affecting organizational intention to adopt forensic accounting practices: A case of Jordan. *Problems and Perspectives in Management*, *21*(3), 334–351. https://doi.org/10.21511/ppm.21(3).2023.27

Alruwaili, W. S., Ahmed, A. D., & Joshi, M. (2023). IFRS innovation, governance practices and firm performance: A new empirical assessment of moderating effects across GCC region. *Equilibrium. Quarterly Journal of Economics and Economic Policy*, *18*(3), 615–659. https://doi.org/10.24136/eq.2023.020

Altawalbeh, M. A. (2023). CORPORATE GOVERNANCE SYSTEMS AND FINANCIAL RISKS: A DEVELOPING COUNTRY EVIDENCE. *Journal of Governance and Regulation*, *12*(3 Special Issue), 232–242. https://doi.org/10.22495/jgrv12i3siart5

Anisykurlillah, I., Januarti, I., & Zulaikha. (2022). THE ROLE OF THE AUDIT COMMITTEE AND EMPLOYEE WELL-BEING IN CONTROLLING EMPLOYEE FRAUD. *Journal of Governance and Regulation*, *11*(4), 168–178. https://doi.org/10.22495/jgrv11i4art16

Arum, E. D. P., Wijaya, R., Wahyudi, I., & Brilliant, A. B. (2023). Corporate Governance and Financial Statement Fraud during the COVID-19: Study of Companies under Special Monitoring in Indonesia. *Journal of Risk and Financial Management*, *16*(7). https://doi.org/10.3390/jrfm16070318

Bader, A. A., Abu Hajar, Y. A., Weshah, S. R. S., & Almasri, B. K. (2024). Predicting Risk of and Motives behind Fraud in Financial Statements of Jordanian Industrial Firms Using Hexagon Theory. *Journal of Risk and Financial Management*, *17*(3), 120. https://doi.org/10.3390/jrfm17030120

Branet, D.-S., & Hategan, C.-D. (2024). Bibliometric Framing of Research Trends Regarding Public Sector Auditing to Fight Corruption and Prevent Fraud. *Journal of Risk and*

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

Financial Management, *17*(3), 94. https://doi.org/10.3390/jrfm17030094

Damayanti, N. N. S. R., & Agustia, D. (2024). Organizational commitment, religiosity, and auditors' responsibility for fraud detection. *International Journal of Management and Sustainability*, *13*(1), 14–25. https://doi.org/10.18488/11.v13i1.3589

De La Torre Lascano, C. M., & Quiroz Peña, J. I. (2023). Cybercrime and its association in the commission of financial fraud in COVID-19 pandemic. *Revista Venezolana de Gerencia*, *28*(102), 609–628. https://doi.org/10.52080/rvgluz.28.102.11

Din, M., Munawarah, M., Ghozali, I., Achmad, T., & Karim, F. (2022). GOVERNANCE OF FINANCIAL MANAGEMENT AND REGULATION-BASED FISCAL ACCOUNTABILITY. *Journal of Governance and Regulation*, *11*(2), 116–123. https://doi.org/10.22495/jgrv11i2art10

Gleason, K., Kannan, Y. H., & Rauch, C. (2022). Fraud in startups: what stakeholders need to know. *Journal of Financial Crime*, *29*(4), 1191–1221. https://doi.org/10.1108/JFC-12-2021-0264

Handayani, S., & Kawedar, W. (2021). Could the minimization of opportunity prevent fraud? An empirical study in the auditors' perspective. *Accounting*, *7*(5), 1157–1166. https://doi.org/10.5267/j.ac.2021.2.023

Hasnan, S., Othman, N., Hussain, A. R. M., & Ali, M. M. (2022). THE INFLUENCE OF FRAUD TRIANGLE FACTORS ON REAL EARNINGS MANAGEMENT. *Journal of Governance and Regulation*, *11*(2), 94–106. https://doi.org/10.22495/jgrv11i2art8

Jamieson, D., Awolowo, I. F., Garrow, N., Winfield, J., & Bhaiyat, F. (2019). FINANCIAL SHENANIGANS: THE IMPORTANCE OF ANTI-FRAUD EDUCATION. *Journal of Governance and Regulation*, *8*(3), 58–63. https://doi.org/10.22495/jgr_v8_i3_p5

Joseph, C., Utami, I., Madi, N., Rahmat, M., Tunga Janang, J., & Omar, N. H. (2021). A Comparison of Online Fraud Prevention Disclosure in Malaysian and Indonesian Public Universities. In *MANAGEMENT AND ACCOUNTING REVIEW* (Vol. 20).

Kassem, R. (2023). External auditors' use and perceptions of fraud factors in assessing fraudulent financial reporting risk (FFRR): Implications for audit policy and practice. *Security Journal*. https://doi.org/10.1057/s41284-023-00399-w

Khatib, S. F. A., Abdullah, D. F., Hendrawaty, E., & Elamer, A. A. (2022). A bibliometric analysis of cash holdings literature: current status, development, and agenda for future research. *Management Review Quarterly*, *72*(3), 707–744. https://doi.org/10.1007/s11301-021-00213-0

Khikmah, S. N., Rohman, A., & Januarti, I. (2023). THE ROLE OF INTERNAL AUDIT AND LEADERSHIP STYLE IN INCREASE OF FRAUD PREVENTION: A STEWARDSHIP THEORY PERSPECTIVE. *Corporate and Business Strategy Review*, *4*(4 Special Issue), 271–278. https://doi.org/10.22495/cbsrv4i4siart8

Kowal-Pawul, A., & Przekota, G. (2021). Importance of VAT digitization for income disclosure in section F- construction – A case for Poland. *Journal of International*

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

Studies, *14*(4), 67–86. https://doi.org/10.14254/2071-8330.2021/14-4/5

Kzykeyeva, A. (2022). Risk-Based Approach to Improving the Quality of Internal Audit. *Quality - Access to Success*, *23*(189), 228–237. https://doi.org/10.47750/QAS/23.189.26

Laupe, S., Abdullah, M. I., Kahar, A., Saleh, F. M., Zahra, F., & Syamsuddin, N. A. (2022). AUDITOR'S SKEPTICISM, FORENSIC ACCOUNTING, INVESTIGATION AUDIT AND FRAUD DISCLOSURE OF CORRUPTION CASES. *Journal of Governance and Regulation*, *11*(3), 189–196. https://doi.org/10.22495/JGRV11I3ART16

Mardjono, E. S., Suhartono, E., & Hariyadi, G. T. (2024). Does Forensic Accounting Matter? Diagnosing Fraud Using the Internal Control System and Big Data on Audit Institutions in Indonesia. *WSEAS Transactions on Business and Economics*, *21*, 638–655. https://doi.org/10.37394/23207.2024.21.53

Martinez-Fernandez, P., DeLlano-Paz, F., Calvo-Silvosa, A., & Soares, I. (2019). Assessing renewable energy sources for electricity (RES-E) potential using a CAPM-analogous multi-stage model. *Energies*, *12*(19). https://doi.org/10.3390/en12193599

Martins, O. S., & Júnior, R. V. (2020). The influence of corporate governance on the mitigation of fraudulent financial reporting. *Revista Brasileira de Gestao de Negocios*, *22*(1), 65–84. https://doi.org/10.7819/rbgn.v22i1.4039

Morales, H. R., Porporato, M., & Epelbaum, N. (2022). Benford's law for integrity tests of high-volume databases: a case study of internal audit in a state-owned enterprise. *Journal of Economics, Finance and Administrative Science*, *27*(53), 154–174. https://doi.org/10.1108/JEFAS-07-2021-0113

Mousavi, M., Zimon, G., Salehi, M., & Stępnicka, N. (2022). The Effect of Corporate Governance Structure on Fraud and Money Laundering. *Risks*, *10*(9). https://doi.org/10.3390/risks10090176

Nonnenmacher, J., & Gómez, J. M. (2021). Unsupervised anomaly detection for internal auditing: Literature review and research agenda. *International Journal of Digital Accounting Research*, *21*, 1–22. https://doi.org/10.4192/1577-8517-v21_1

Nurcahyono, N., Hanum, A. N., Kristiana, I., & Pamungkas, I. D. (2021). Predicting fraudulent financial statement risk: The testing dechow f-score financial sector company inindonesia. *Universal Journal of Accounting and Finance*, *9*(6), 1487–1494. https://doi.org/10.13189/ujaf.2021.090625

Parluhutan, C. A., Ermawati, & Widyastuti, S. (2022). The Influence of Auditor Ethics, Auditor Motivation, Locus of Control on Audit Quality: Role of Professional Skepticism. *Universal Journal of Accounting and Finance*, *10*(1), 267–275. https://doi.org/10.13189/ujaf.2022.100127

Putra, I., Sulistiyo, U., Diah, E., Rahayu, S., & Hidayat, S. (2022). THE INFLUENCE OF INTERNAL AUDIT, RISK MANAGEMENT, WHISTLEBLOWING SYSTEM AND BIG DATA ANALYTICS ON THE FINANCIAL CRIME BEHAVIOR PREVENTION. *Cogent Economics and Finance*, *10*(1). https://doi.org/10.1080/23322039.2022.2148363

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412

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

Sánchez Henríquez, J. A., Neira Cortés, P., & Severino González, P. (2022). Fraud: A global look at its conceptual development. *Revista Venezolana de Gerencia*, *27*(99), 884–910. https://doi.org/10.52080/rvgluz.27.99.3

Sari, M. P., Mahardika, E., Suryandari, D., & Raharja, S. (2022). The audit committee as moderating the effect of hexagon's fraud on fraudulent financial statements in mining companies listed on the Indonesia stock exchange. *Cogent Business and Management*, *9*(1). https://doi.org/10.1080/23311975.2022.2150118

Suryandari, N. N. A., Yadnyana, I. K., Ariyanto, D., & Erawat, N. M. A. (2023). Determinant of fraudulent behavior in the Indonesian rural bank sector using the fraud hexagon perspective. *Banks and Bank Systems*, *18*(4), 181–194. https://doi.org/10.21511/BBS.18(4).2023.16

Sushkov, V. M., Leonov, P. Y., Nadezhina, O. S., & Blagova, I. Y. (2023). Integrating Data Mining Techniques for Fraud Detection in Financial Control Processes. *International Journal of Technology*, *14*(8), 1675– 1684. https://doi.org/10.14716/ijtech.v14i8.6830

Yami, N., & Poletti-Hughes, J. (2022). Financial Fraud, Independent Female Directors and CEO Power. *Journal of Risk and Financial Management*, *15*(12). https://doi.org/10.3390/jrfm15120575

Yaqoub, M., Hamad, S., Alhammadi, H., Elkelish, W. W., Abdalla, Y. A., & Hussain, A. (2023). UNDERSTANDING ACCOUNTING FRAUD MOTIVATION, PROTECTION PROCEDURES, AND FIRMS' PERFORMANCE: EXTERNAL AUDITORS' PERSPECTIVE. *Corporate Governance and Organizational Behavior Review*, *7*(3), 19–26. https://doi.org/10.22495/cgobrv7i3p2

E-ISSN 2581-1088
DOI: 10.25124/jaf.v9i2.9412