



ADVANCED INTERNATIONAL JOURNAL
OF BUSINESS, ENTREPRENEURSHIP
AND SMES
(AIJBES)

www.gaexcellence.com/aijbis



THE EFFECTIVENESS OF ETHICAL CULTURE, INTERNAL CONTROL, AND INFORMATION TECHNOLOGY SYSTEMS ON OCCUPATIONAL FRAUD IN SMES: EMPLOYEES' PERSPECTIVE

Nadiah H. Saharudin¹, Mazurina Mohd Ali^{2*}, Noor Hasniza Haron³, Suhaily Hasnan⁴

¹ SME Banking, Menara Maybank, Kuala Lumpur, Malaysia

 nadh2810@gmail.com



<https://orcid.org/0009-0008-8442-3196>

² Faculty of Accountancy, Universiti Teknologi MARA, Cawangan Selangor, Kampus Puncak Alam, Selangor, Malaysia

 mazurina@uitm.edu.my



<https://orcid.org/0000-0002-2877-3414>

³ Faculty of Accountancy, Universiti Teknologi MARA, Cawangan Selangor, Kampus Puncak Alam, Selangor, Malaysia

 hasniza3330@uitm.edu.my



<https://orcid.org/0000-0001-5046-3802>

⁴ Faculty of Accountancy, Universiti Teknologi MARA, Cawangan Selangor, Kampus Puncak Alam, Selangor, Malaysia

 suhailyhasnan@uitm.edu.my



<https://orcid.org/0000-0002-6050-8741>

*Corresponding Author

Article Info:

Article history:

Received date: 07.07.2026

Revised date: 22.07.2026

Accepted date: 24.08.2026

Published date: 30.09.2026

To cite this document:

Saharudin, N. H., Ali, M. M., Haron, N. H., & Hasnan, S. (2026). The Effectiveness of Ethical Culture, Internal Control, and Information Technology Systems on Occupational Fraud in SMEs: Employees' Perspective. *Advanced*

Abstract:

The purpose of this study is to examine the effectiveness of fraud prevention mechanisms, namely, ethical culture, internal control, and information technology systems, in preventing occupational fraud in SMEs. Questionnaires were distributed to 500 employees in SMEs in the Klang Valley to obtain the required data. From the original 500 distributed questionnaires, 133 usable responses were returned. The analyses conducted were descriptive, reliability, normality, Pearson correlation coefficient, and multiple regression analyses. The results found significant relationships between ethical culture, information technology systems, and occupational fraud. These results show that employees perceived ethical culture and information technology systems as the most effective fraud prevention mechanisms. Meanwhile, it is quite interesting that internal controls are not deemed a useful tool despite various studies emphasising the formulation of strong internal controls as a mechanism to curb potentially fraudulent activities. This study has potential benefits to SME owners, managers, employees, and policymakers as they work to improve the effectiveness

International Journal of Business Entrepreneurship and SMEs, 8 (29), 2003-2029. of fraud prevention mechanisms by enhancing the ethical culture and information technology system.

DOI: 10.35631/AIJBS.829115 **Keywords:**

Ethical Culture, Fraud, Information Technology, Internal Control, Risk, SMEs



© The authors (2026). This is an Open Access article distributed under the terms of the Creative Commons Attribution (CC BY NC) (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited. For commercial re-use, please contact aijb@gaexcellence.com.

Introduction

Occupational fraud may take a variety of forms, ranging from the simple theft of corporate assets to the more complex manipulation of financial accounts (Wells, 2017). Typically, occupational fraud occurs when a corporation lacks specialised oversight. According to the Association of Certified Fraud Examiners' (ACFE) (2022) Report to the Nation, about 44% of occupational fraud happened in private companies, followed by 25% in publicly listed companies. The mean losses equal USD 138,000 for both types of organisations. This figure indicates that perpetrators from small and medium-sized enterprises would have more opportunities to commit fraud due to insufficient fraud prevention mechanisms (Ali et al., 2020). Fraud activities, such as billing and payroll fraud, frequently happen in small businesses, with check and payment tampering occurring four times more often (ACFE, 2022). The survey by ACFE (2022) of 2,504 cases in 125 countries indicated that organisations risk losing 5% of their revenue to occupational fraud. In this regard, small businesses are particularly vulnerable and experience a higher percentage of the median loss compared to larger firms (Kramer, 2015; Sow et al., 2018b). Over the years, there is no specific way to eliminate fraud, regardless of the organisation's size, and no sector of the economy is safe from its impacts (Krambia-Karpadis & Zopiatis, 2010).

The perpetrator of occupational fraud can come from any occupational position (Omar et al., 2016). According to ACFE (2022), although 20% of occupational fraud is committed by owners/executives, they constituted the most significant losses, with a mean of USD 600,000. In contrast, the fraud by managers and employees contributed to losses, with a mean of USD 150,000 and USD 60,000, respectively. The involvement of senior management in occupational fraud stems from their ability to conspire or override internal controls, relating to the capability and opportunity elements in the fraud hexagon theory. This is consistent with Krambia-Karpadis & Zopiatis (2010), who asserted that employee fraud is more common than third-

party and management fraud. Nevertheless, Sow et al. (2018a) contended that significant fraud perpetrators are third parties, including former employees, suppliers, and customers. This study focused on small and medium enterprises (SMEs) because they represent the backbone of the Malaysian economy. In the Malaysian context, SMEs are typically defined based on their annual sales turnover and number of full-time employees (SME Corp, 2020). The category of the respective SME segments is presented in Table 1 below:

Table 1: SME Categories

Sector Size	Manufacturing	Services & Other Sectors
Medium	Sales Turnover: RM15M $\leq$ RM50M OR Employees: From 75 to $\leq$ 200	Sales Turnover: RM3M $\leq$ RM20M OR Employees: From 30 to $\leq$ 75
Small	Sales Turnover: RM300,000 < RM15M OR Employees: From 5 to < 75	Sales Turnover: RM300,000 < RM3M OR Employees: From 5 to < 30
Micro	Sales Turnover: < RM300,000 OR Employees: < 5	Sales Turnover: < RM300,000 OR Employees: < 5

Source: SME Corp (2020)

SMEs constitute 97.2% of business establishments in Malaysia, with 85.5% operating in the services sector, contributing 38.2% to GDP and employing 7.25 million workers (SME Corp, 2020). Of the 1.15 million SMEs, 78.4% are micro, 20.0% are small, and 1.6% are medium-sized enterprises. In promoting good governance, the Malaysian Code of Corporate Governance (MCCG) emphasises transparency, accountability, and integrity, including effective internal control, risk management, and internal audit functions. These mechanisms strengthen fraud prevention and detection by identifying and mitigating risks and enhancing the transparency and timeliness of financial information.

As far as this study is concerned, there is no generalised code of business conduct specifically tailored to SMEs, potentially contributing to weaker anti-fraud measures and greater fraud vulnerability than larger corporations (Ali et al., 2020). Technological advancement and increasingly sophisticated fraud techniques further expose Malaysian SMEs to fraud risks (Shanmugam & Ali, 2012). Although prior research has examined fraud prevention from the perspectives of managers and supervisors (Sow et al., 2018b), limited studies have assessed the effectiveness of anti-fraud mechanisms from employees' perspectives. Gunasegaran et al. (2018), for instance, examined fraud prevention mechanisms in three medium-sized enterprises, focusing primarily on internal control. This gap highlights the need for further empirical research on fraud prevention mechanisms in Malaysian SMEs from the employees' perspective.

The focus of this study is to examine the effectiveness of fraud prevention mechanisms adopted (i.e., ethical culture, internal control, and information technology systems) by SMEs on occupational fraud. This study is expected to enhance academic literature by providing empirical evidence regarding the effectiveness of fraud prevention mechanisms from the perspective of employees within SMEs. This approach can pose a unique point as it incorporates the perceptions and experiences of those working within these organisations,

potentially shedding light on previously unexplored aspects of fraud prevention. As employees play a critical role in preventing fraud, their perceptions can significantly influence the success of these measures. Apart from that, this study would benefit and assist relevant authorities, policymakers, and the government in improving modules on the effectiveness of fraud prevention measures. This contribution is valuable, particularly for organisations such as the Companies Commission of Malaysia (CCM) and SME Corporations, which provide essential training and modules to SME owners. Ultimately, this study may assist SME owners and managers in assessing the effectiveness of their fraud prevention measures and resolving any weaknesses that the companies face.

The remainder of this paper is structured as follows: the next part presents the literature review and hypotheses development, followed by research methods and design, and the discussion of the results and analysis of this study. This paper presents suggestions for future research in the conclusion section.

Literature Review and Hypotheses Development

Occupational Fraud in Small and Medium Enterprises (SMEs)

Occupational fraud is a type of white-collar crime in which persons knowingly commit fraud against the organisation that employs them (Nawawi & Salin, 2018). Omar et al. (2016) evoked that newly established firms are more susceptible to fraud because it lacks a well-organised operating structure and have insufficient internal controls. In Australia, occupational fraud is increasingly posing a significant criminal threat to the country's socio-economic fabric. Azjen (1991) further suggested that the act of occupational fraud requires an employee to have a specific motivation for his or her actions. While most employees can resist the temptation to commit fraud, some may yield if both the incentive and opportunity exist within the organisation (Azjen, 1991). Therefore, the internal controls must be frequently reviewed and updated to ensure their effectiveness in combating any fraud incident in the organisation.

Occupational fraud can be categorised into three primary categories: asset misappropriation, financial statement fraud, and corruption. Firstly, asset misappropriation involves misusing an organisation's assets for personal gain, including activities such as stealing company cash, using office equipment for personal use, or colluding with outsiders to commit fraud. According to Albrecht et al. (2008), for asset misappropriation to happen, the “act” of asset theft, concealment and conversion must all be present. Further, the assets should have been taken for the personal benefit of the individuals misappropriating the assets, and such individuals could be the organisation's employees, customers, or vendors, or individuals who neither work for nor work in the organisation (Albrecht et al., 2008). The ACFE's 2022 Report to the Nations classified asset misappropriation into two main types: cash misappropriation and misappropriation involving inventory and other assets, with five identified misappropriation schemes, including cash theft, skimming, fraudulent disbursements, check tampering, and register disbursements. They are the easiest forms of fraud to commit (Padget, 2014) and can involve individuals at all levels within a firm (Zahari et al., 2020). They account for 86% of fraud cases, with a median loss of USD 100,000 (ACFE, 2022). Secondly, financial statement fraud is the least common, but is also the most expensive, with a reported median loss of USD 593,000 (ACFE, 2022). It involves deliberate misstatements or omissions in financial statements to mislead users. Thirdly, corruption is the most widespread form of occupational

fraud globally, encompassing bribery, conflicts of interest, extortion, and the illegal use of public authority for personal gain (Siddiquee, 2010; ACFE, 2022).

Past studies indicated that small businesses will be severely burdened by a lack of expertise and financial resources (Gunasegaran et al., 2018; Zainal et al., 2022). Implementing anti-fraud measures, such as regular audits and employee background checks, is crucial for SMEs to mitigate the risk of fraud and its detrimental impact on the organisation (Power, 2013). Employees in SMEs will not be deterred or fearful of being caught if there is no internal auditing staff in place to prevent them from taking advantage of the opportunity to commit fraud. Some SMEs lack in-house accountants (Zainal et al., 2022) and resort to hiring part-time account clerks to maintain financial records. Alternatively, they would hand over all relevant documents to an accounting firm for processing for tax filing or preparing financial statements, such as the audit report (Ali et al., 2023). Furthermore, not all business owners have an accounting background. They have various levels of education, which is another personal factor that may expose the company to fraud if there is insufficient internal control and management procedures in place. Financial difficulties in the business, low ethical culture, lack of internal control, advancement of technology, and legal issues are among the factors that contribute to occupational fraud.

Fraud Hexagon Theory

Cressey's (1953) Fraud Triangle theory is a widely used fraud theory, identifying three factors contributing to fraud: incentives or pressures, opportunities, and rationalisation. It posits that financial pressure is a motivating factor for fraud, perceived opportunity arises from weak internal controls, and a belief in evading detection and rationalisation involves justifying fraudulent behaviour. This theory implies that all three factors must be present for fraud to occur, providing a framework for understanding and preventing fraudulent behaviour by addressing motivations, opportunities, and justifications. The traditional fraud triangle model mainly focuses on individuals acting alone (Dorminey et al., 2012). However, as fraud methods evolve, some experts anticipate the emergence of a new class of occupational offenders who may not resist temptation due to a lack of moral fortitude. Dorminey et al. (2012) examined the fraud triangle and acknowledged its utility in assessing fraud risk. Still, they also argued that the model alone might be insufficient for deterring, preventing, and detecting fraud effectively in contemporary contexts. Fraud is a complicated process that is always changing to fit the current situation. It changes over time and has many different parts. So, the procedures, processes, and internal controls that the company already have, need to be reviewed often. To this end, this study used the fraud hexagon theory elements, with the acronym SCCORE (i.e., stimulus, capability, collusion, opportunity, rationalisation, and ego) (Vousinas, 2019) as presented Table 2 below:

Table 2: Fraud Hexagon Theory Elements

Elements	Explanation
Stimulus	The pressure to commit fraud arises from the desire to gain financial or non-financial incentives, which can take various forms, such as financial needs, performance targets, or the wish to exploit or outwit the system. In this study, the incentive represents the illicit gain that perpetrators seek through occupational fraud.

Capability	Personal traits and abilities motivate fraud perpetrators. An opportunity presents the potential for fraud, with rationalisation and incentives driving them toward it. However, the perpetrator needs the capability to exploit this opportunity. The ACFE survey in 2022 revealed that while small companies may lack internal controls, larger companies are more likely to override these controls. This underscores the significance of capability and opportunity in circumventing established internal controls within organisations.
Collusion	The rise in fraud incidents is evident in ACFE's (2020b) survey, which revealed that cases involving multiple perpetrators had a higher median loss compared to single-perpetrator cases. In their study, 51% of fraud incidents involved at least two perpetrators, and these cases had a significantly higher median loss. A single perpetrator typically resulted in a median loss of USD 90,000, while cases with two perpetrators had a median loss of USD 105,000. When collusion involved more than three perpetrators, the median loss escalated to USD 350,000.
Opportunity	The ability to commit fraud stems from the perpetrator's belief that they can devise and execute fraudulent acts without being caught. Numerous studies highlight the connection between opportunity and an individual's role and authority within the organisation.
Rationalisation	The justification of fraudulent acts is the way a perpetrator rationalises their behaviour to reduce feelings of guilt. In the context of this study, it reflects an individual's values and how they justify their wrongful actions. A strong ethical culture within the organisation can help minimise such rationalisation.
Ego	Ego, described as power over people or situations (Duffield & Grabosky, 2001), encompasses a sense of superiority, mastery, and the desire for admiration from others (Weisburd & Waring, 2001). Personality, which characterises an individual, is identified by Geis (2011) as the most influential factor for committing fraud. In this study, the most common motives for fraud are the sense of entitlement and the desire for power. Kranacher et al. (2010) emphasised ego as a significant motivation for fraud, while Pedneault et al. (2012) contended that a perpetrator must possess a strong ego and great confidence that their fraudulent actions or gains will remain undetected.

Fraud Prevention Mechanism

Fraud prevention is one of the most important controls before a crime (Rashid et al., 2022). According to Bishop (2004), management must balance fraud prevention and detection. However, Gunasegaran et al. (2018) stated that Malaysian SMEs have limited fraud prevention mechanisms. As argued by Kramer (2015), larger corporations have better fraud prevention and detection mechanisms since their resources can accommodate having their own internal audit department and hiring more employees in the accounting department that can cater for different roles and functions. He also argued that small businesses viewed implementing control or preventive measures as neither a cost advantage nor increasing the company's revenue. Mat et al. (2013) noted that companies allocate a significant portion of resources to fraud detection (80%) rather than prevention (20%). Companies that lack fraud prevention and

detection mechanisms are more likely to face challenges in terms of business viability and competitiveness and may even face closure because of inadequate structure, plans, and policies (Gunasegaran et al., 2018). Despite consistent implementation, adoption rates of anti-fraud controls have remained steady over the past decade. ACFE (2022) had listed the 18 common anti-fraud controls that comprises of external audit of financial statements, code of conduct, internal audit department, management certification of financial statements, external audit of internal controls over financial reposting, management review, hotline, independent audit committee, anti-fraud policy, employee support programmes, fraud training for employees, fraud training for managers/executives, dedicated fraud department, formal fraud risk assessments, surprise audits, proactive data monitoring/analysis, job rotation/mandatory vacation and rewards for the whistleblower. Other studies have included hotlines, anti-fraud policies, and fraud training for employees/managers and executives as part of the anti-fraud control mechanisms. Although past studies have examined many of these controls, none have given specific definitions of the control mechanisms.

Ethical Culture

Ethical culture refers to how an organisation demonstrates its values, mostly about doing the right things or the right way of doing things expected from the employees. It is a pattern of shared beliefs that new members are taught to understand and adopt (Schein, 1985). Ethical culture is perceived as one way to influence the intention to report unethical behaviour of employees and managers. Nevertheless, situational factors can affect it, alongside personal factors like age, education, and gender (Murphy & Dacin, 2011). For instance, newly hired employees would be less likely to report unethical behaviours as they are just trying to get used to the company's environment, and those anticipating promotions might choose to remain silent to avoid affecting their career advancement. Thus, they would rather not speak up on truthful matters. One of the most common ethical cultures is building a culture of honesty and integrity. Fraud prevention mechanisms are correlated with an effective culture of honesty (Sow et al., 2018b). Companies that prioritise and uphold strong ethical values are more likely to not only attract investors but also retain their customer base. This correlation is further supported by Barlaup et al. (2009), which stated that only firms with an ethical culture might survive in the long run due to their ability to attract stakeholders. The study also highlighted that investors tend to prefer companies led by trustworthy individuals. According to Murphy and Dacin (2011), unethical behaviour of employees is most likely due to the failure of top management to promote good traits. Thus, establishing an honesty culture allows top management to identify and define acceptable ethical behaviours and effectively communicate these standards to their employees (Sengur, 2012).

Top management plays a vital role in adopting good ethical values, as it should be a top-down approach. Management must lead by example to ensure the effectiveness of ethical culture as a part of fraud prevention measures. Based on auditors' experiences, management attitudes are more important in mitigating controls than other fraud incentives and opportunities (Hernandez & Groot, 2007). While internal controls are central to fraud prevention, the way management communicates and interacts with them can either strengthen or weaken their effectiveness (Agarwal & Kallapur, 2018). For instance, the board of directors plays a positive role in instilling an organisational culture of ethics and articulating it clearly to every employee, including adopting policies to set a positive culture of behaviour driven by 'tone at the top' (Omar & Bakar, 2012). Effective communication in conveying messages will minimise the issue of employees being unaware or not well informed about specific policies and procedures

(Nawawi & Salin, 2018). According to Higgins (2011), creating an integrity culture is the highest-ranking of anti-fraud strategies. This culture is primarily shaped by leadership attitudes and choices, not by processes. Thus, integrity must be a critical component of the executive search equation; it must be constantly developed at the individual and executive team levels. It must be regarded as a prerequisite for advancement and compensation. Failing to prioritise integrity means addressing only the symptoms rather than the root causes of fraud. It is argued that, even though the company has created its own organisational culture, a corporate culture lenient towards fraud can help rationalise an act of occupational fraud (Kumar et al., 2018). Further, unlike other research studies, Halbourni et al. (2016) found that the culture of honesty has a low positive impact on fraud prevention and detection for UAE companies.

According to previous research, organisational culture can critically influence employee attitudes towards fraud (Somers, 2001; Kawiana et al., 2018; Li, 2015; Pfister, 2009; Davis & Pesch, 2013). However, there has been limited research to identify how organisational culture specifically affects the likelihood of occupational fraud occurring within an organisation. While several scholars appear to agree on the significant influence of corporate culture in deterring potential fraud, the existing literature on occupational fraud research is viewed as lacking in this field, and mostly for logical reasons. It is suggested that any research aiming to establish the link between organisational culture and the probability of occupational fraud should involve a strong multidisciplinary team (Kumar et al., 2018). According to Zakaria et al. (2016), the embeddedness of essential values among employees is essential because audit procedures alone do not guarantee that fraud would be detected even if the audit is performed with professional care. There is no consistent measure to determine the codes of conduct. For instance, management accountants in the United States were surveyed using a single-item measure of codes of conduct (Somers, 2001). The respondents were given three options, 'Yes', 'No', or 'I don't know', to the statement whether their companies had a written code of conduct for their employees. The application of codes of conduct can assist managers in maintaining integrity and providing a better justification for avoiding bribery (Le et al., 2021). Honest employees are more likely to report suspicious activities without fear of retaliation. In addition to internal staff, an anonymous hotline should be established and extended to include suppliers, customers, and vendors (Kramer, 2015).

Sow et al. (2018a) recommended that SMEs' managers and owners develop their own business conduct policies. The policies must be communicated effectively to all employees to raise awareness and understanding. Le et al. (2021) emphasised that effective internal control implementation reduces employee rationalisation when faced with fraud opportunities. A company's core values and behavioural guidelines, at the very least, make it difficult for the employees to claim that they were unintentionally involved in fraudulent activities. Fraud prevention is correlated with fostering a culture of honesty (Sow et al., 2018b). Companies with a strong ethical culture are more likely to attract investors and retain customers (Barlaup et al., 2009). They emphasised that only firms with an ethical culture can thrive long-term, as they can attract stakeholders, and investors prefer businesses led by trustworthy individuals. Murphy and Dacin (2011) suggest that unethical employee behaviour often results from top management's failure to promote good traits. Thus, by establishing a culture of honesty, top management could identify acceptable ethical behaviours and efficiently communicate them to the subordinates (Parthiban et al., 2026; Sengur, 2012).

Companies with ethical behaviour have a greater chance of long-term survival and retaining stakeholders (Barlaup et al., 2009). In the Malaysian work environment, cultural values such

as respect for the elderly, non-assertiveness, hierarchy, non-aggressiveness, relationships, and trust have been integrated. Consequently, establishing a culture of honesty is a primary endeavour in preventing corporate fraud (Sengur, 2012). While previous studies have proposed different ethical cultures for fraud prevention, this study specifically focuses on assessing the effectiveness of such cultures from employees' perspectives. Hence, the hypothesis of this study is as follows:

H1: There is a significant negative relationship between the effectiveness of ethical culture and occupational fraud from the employees' perspective.

Internal Control

The Committee of Sponsoring Organisations of the Treadway Commission (COSO) (2019) defined internal control as a process involving an entity's board of directors, management, and personnel to reasonably ensure objectives in operational effectiveness, financial reporting reliability, and compliance with laws and regulations. According to the COSO framework, the control environment sets the organisation's tone, and a robust control environment enhances other control components. Conversely, a poor environment weakens other elements, rendering them ineffective. In such situations, control procedures may be disregarded or overridden, creating opportunities for fraud (Peltier-Rivest & Lanoue, 2011). There are a few weaknesses that contribute to ineffective internal control and lead to occupational fraud in an organisation. As listed in the survey conducted by ACFE (2022), the weaknesses were due to lack of internal controls (32%), overriding existing internal control and lack of management review (18% percent, respectively), poor tone at the top (10%), lack of competent personnel in oversight roles (6%), lack of independent checks/audits (5%), lack of employee fraud education (3%), lack of clear lines of authority (2%), and lack of reporting mechanism (less than 1%).

The organisation needs to understand the root cause of fraud and learn effective fraud prevention techniques to safeguard its assets and reputation. Organisations need to move to new or better controls as fraud techniques evolve. Internal control and codes of conduct are crucial not just in developed countries (Lämsiluoto et al., 2016; Lawson et al., 2017), but also in emerging economies (Le et al., 2021). Most studies on internal control have been conducted in developed countries where formal internal control is mandatory for most firms (Chalmers et al., 2019) and where breaches of the law are not socially acceptable (Khan, 2006). In contrast, the role of internal control systems in developing countries may be less clear due to the social acceptance of law violations and the prevalence of corruption (Khan, 2006; Nguyen et al., 2016). Zakaria et al. (2016) examined how internal control affects fraud activities using a case study of a Malaysian oil and gas company. They found that internal control weaknesses played a significant role in facilitating fraud. Internal auditors, however, faced challenges in detecting fraud, as their expertise is not on par with that of those specifically tasked with detecting and investigating fraud. Rahman et al. (2019) argued that internal control's influence in anti-corruption initiatives had been overlooked in previous research.

Occupational fraud can be minimised by setting up an appropriate internal control system, including segregation of duties, proper documentation, proper approvals, and validation of transactions in the organisation (Sow et al., 2018a). Companies need to provide clear job descriptions to staff, ensuring they understand their responsibilities and objectives. Segregation of duties is deemed essential, including policies to be implemented in the organisation. These policies should be clearly explained to employees and restrict access to specific workplaces and authorised personnel (Omar et al., 2016).

According to Nawawi and Salin (2018), poor supervision would lead to abuse and misconduct. It includes the absence of checks and balances that allows employees to exert too much power, control, and authority in making decisions on behalf of the company. As a result, it is necessary to ensure that employees' tasks are closely monitored. Regular and close monitoring of employees' tasks is essential to address any issues promptly (Omar et al., 2016). On the other hand, the process of pre-screening candidates is deemed necessary as it may deter a fraud perpetrator from applying for any position in the company. Background checks, although not foolproof, help identify financial pressures that job seekers may face (Kramer, 2015). This background check is part of due diligence to know the background of the candidate beforehand. Before letting a fraudster in through the front door, a background verification should be conducted throughout the recruiting process to find any red flags in the perpetrator's history. Employment history, criminal checks, reference checks, education verification, credit checks, and drug screening are examples of background checks that the human resources department or interviewers can use during the recruitment process. According to ACFE (2022), 52% of the companies that participated in the survey found red flags during background checks, and unexpectedly, 13% of these companies went ahead and hired the fraudster. Bressler and Bressler (2007) indicated that small businesses and non-profit organisations are reticent to conduct background and reference checks, considering the cost and time involved.

Internal control systems that are well-implemented would reduce the likelihood of fraud. Weak internal controls are commonly identified as a contributing factor to fraud (Dellaportas, 2013; Lokanan, 2014; Zakaria et al., 2016). Firms that have strong internal control systems find it easier to detect and prevent fraud because their corporate governance and anti-fraud functions are more effective. However, as Le et al. (2021) argued, even with strong internal control systems in place, there is still a potential for fraud. This possibility would allow the management team to assess and re-analyse the key factors and identify the responsible individuals or procedures for future correction and enhancement. Hence, improving the efficiency and effectiveness of fraud prevention mechanisms is an ongoing, iterative process rather than a one-time effort. Control procedures are frequently overridden or ignored in a poor environment, creating opportunities for fraud (Peltier-Rivest & Lanoue, 2011). The role of internal control systems may be vague in developing countries due to law violations being generally accepted and prevailing corruption (Khan, 2006; Nguyen et al., 2016). Zakaria et al. (2016) investigated how internal control flaws significantly contribute to fraud in a Malaysian oil and gas company. However, internal auditors may struggle to detect fraud due to their limited expertise compared to those specifically tasked with fraud detection and investigation. Rahman et al. (2019) argued that the influence of internal control on anti-corruption initiatives has been overlooked in prior research.

The COSO internal control model emphasises creating effective internal control through five components that facilitate the achievement of business objectives. This model aims to establish robust internal control, continuously monitor it, and promptly address any issues. Strong internal control is seen as a deterrent to fraud, increasing the likelihood of catching offenders. Effective internal control is essential for organisations of all sizes and types to prevent fraud, detect embezzlement, and ensure the production of accurate and timely financial reports. Hence, the second hypothesis of this study is as follows:

H2: There is a significant negative relationship between the effectiveness of internal control and occupational fraud from the employees' perspective.

Information Technology System

Information technology (IT) encompasses hardware and software technologies for collecting, transmitting, analysing, interpreting, storing, organising, and utilising data effectively. It plays a crucial role in occupational fraud prevention by enabling the provision of reliable and accurate information to users (Suryanto, 2016). However, Simha and Satyanarayam (2016) pointed out that the emergence of sophisticated information technologies has also given rise to new forms of digital fraud schemes. Cyber-criminal prosecutions have doubled from 8% in 2018 to 16% in 2020, with only 45% of Malaysian respondents reporting a dedicated cybercrime combat programme (ACFE, 2022). However, an effective anti-fraud programme is not reliant on a single technology or tool. Many companies struggle to prioritise technology due to limited resources and expertise. Business owners should stay vigilant about advancements in computer-related fraud, especially in information-processing technologies. The growth of internet-related technology has increased vulnerability to external threats, and many SMEs lack the technical knowledge to mitigate these risks. Utilising up-to-date anti-virus software is recommended for data protection, and it should be updated regularly. Additionally, developing specialised security systems and applications is crucial for safeguarding against cyber threats (Koryono, 2013).

Since hacking and data breaches are becoming more common, organisations should proactively consider breach management. Key steps include compiling operation logs and implementing network segregation to limit unauthorised access. Employing fraud control measures, such as requiring multiple approvals for account creation or payee setup, can enhance internal control with appropriate IT systems. IT, while beneficial, presents security and data loss risks, necessitating clear IT controls, including regulations, system development, and physical and online security (Claudia, 2014). Furthermore, deploying suitable financial accounting software can help minimise fraud attempts in financial reporting and ensure timely report preparation. Despite the shift towards digital payments and technology-based businesses, the methods used by fraudsters to obtain illicit gains remain largely consistent (ACFE, 2022). There is a significant correlation, leading to a positive impact on adopting IT and traditional methods in preventing and detecting occupational fraud (Halbouni et al., 2016). Research conducted by Huslina and Islahuddin (2015) on the efficiency of fraud prevention systems in the Banda Aceh government showed that efficiency is notably influenced by the integrity, competence of personnel, and IT usage. Scholars generally believe that a robust internal control system improves efficiency, effectiveness, information reliability, and legal compliance (Lawson et al., 2017). While a culture of honesty has a minor positive impact on fraud prevention and detection in the United Arab Emirates (Halbouni et al., 2016), both IT and traditional methods aim to prevent and detect fraud. Therefore, senior management and the board of directors must recognise the importance of adopting systematic fraud investigation approaches.

Arens et al. (2017) argued that information technology has the potential to improve a company's internal controls and overall risk management, but it also introduces new risks, such as those related to hardware and data security, or the potential introduction of new types of errors that rely too heavily on hardware and software capabilities. Nevertheless, since both IT and traditional methods serve the same purpose, which is to prevent and detect fraud, senior management and the board of directors must be made aware of the need to adopt systematic fraud investigation approaches. The application of IT would help companies produce accurate and updated information such as financial reports, which would greatly prevent fraud in the organisation (Suryanto, 2016). Hence, the third hypothesis of this study is as follows:

H3: There is a significant negative relationship between the effectiveness of information technology systems and occupational fraud from the employees' perspective.

Research Method and Designs

Sample Selection and Research Instrument

The population of this study is SMEs in Malaysia, particularly in the Klang Valley region. The sample of this study included business owners and employees at all levels in the organisation structure because individuals at different levels would have different perspectives and knowledge of fraud prevention mechanisms in their company. Therefore, the unit of analysis is an individual from each SME. A simple random sampling technique was used to select the sample units where all individuals had a known and equal chance of being selected. At the time this study was conducted, the total number of registered SMEs (this study's population) in Malaysia was 1,151,339. Based on Sekaran and Bougie (2016), for a population of more than 1,000,000, the sample size required for this study to be plausible and viable is 384 individuals. This study used a structured survey questionnaire distributed online. Online distribution allows potential respondents ample time to respond. To obtain a higher response rate, this study assured the respondents that all information provided would be confidential. The structured questionnaire was designed simply and written in dual language (English and Malay). The respondents could choose to complete the questionnaire in their preferred language. The questionnaire consisted of 53 questions, divided into seven (7) sections. Section A introduces the researcher and explains the broad objective of the survey. Sections B (in English) and C (in Malay) relate to the general information or personal characteristics of the respondents, such as gender and age. Section D is about perceptions of the type of occupational fraud encountered in the organisation. Section E is about perceptions of the effectiveness of ethical culture, while Section F is about perceptions of internal control and information technology systems. The statements were mostly self-developed based on "The Fraud Tree – Occupational Fraud and Abuse Classification System", Fraud Prevention Checklist (ACFE, 2022). The questionnaire was pre-tested for clarity and reliability of the statements and questions related to the variables used (Sekaran & Bougie, 2016).

According to Sekaran and Bougie (2016), a five-point or seven-point scale with anchors is an itemised scale that allows respondents to determine their closest option to the items given. This measurement is widely used in business research. Therefore, this study adopted a five-point Likert scale in the questionnaire to determine the respondents' perceptions of the effectiveness of fraud prevention mechanisms in their organisations. For Sections D to G, the Likert scale is '1' (Strongly Disagree), '2' (Disagree), '3' (Slightly Agree), '4' (Agree), and '5' (Strongly Agree). There are three (3) questions in each section that required the respondents to analyse the effectiveness of the fraud prevention mechanisms using the numerical scale '1' (Completely Ineffective), '2' (Ineffective), '3' (Slightly Effective), '4' (Effective), and '5' (Completely Effective).

Data Collection

This study used primary data using questionnaires, which were distributed to 500 potential respondents comprising of business owners and employees on a staggered basis. This was to monitor the progress of the responses. The link to the questionnaires was shared using online platforms, specifically WhatsApp and email. Regarding data collection, a study in the

Malaysian context found that the response rate of a survey is low, ranging from 10% to 20% (Eltayeb et al., 2011). Based on the experience of previous researchers, this study decided to distribute more questionnaires than the suggested sample; therefore, 500 questionnaires were distributed to respondents with an expected return of 20%. Hence, a minimum of 100 responses should be received to achieve significant statistical results. On top of that, this approach considered the possibility of incomplete responses and questionnaires not returned. The actual number of individuals that responded to this survey was 154 (30.8%). Upon excluding the responses from non-SME employees, a total of 133 responses (26.6%) were usable for this research. The number of responses received was acceptable despite two reminders given through WhatsApp and emails.

Results and Discussion

Demographic Profile of Respondents

The total number of respondents for this study was 133. Table 3 presents the descriptive analysis of the respondents' demographic profiles. The results show that the gender distribution is almost equal, with 50.4% male respondents and 49.6% female respondents. Further, most respondents are executives/clerks (58.6%), and the remaining 41.4% are business owners/directors. From the age group perspective, 51.1% of the respondents are between 30-39 years old, 18.8% between 40-49 years old, and 16.5% between 50-59 years old. Table 3 also shows the educational background of the respondents, where 13.5% have a diploma, 57.9% graduated with a bachelor/Degree, followed by 6.8% having a professional certificate, and 16.5% having a Master/PHD qualification. Most respondents have more than one year of experience working in the same organisation, with 35.3% having 1-5 years of working experience, 33.1% having 6-10 years of working experience, and 11.8% serving the organisation for 11-20 years. The entity types that the respondents are currently working in are private limited companies (64.7%), followed by sole proprietorships and professional entities (11.3%, respectively), and partnerships (9.0%). The respondents are working in different types of business, and the majority of them are from services (24.80%), followed by others (23.30%), professional services (16.50%), and retailer/wholesaler (13.50%). On top of that, the respondents have estimated the number of employees in their company, with the majority of them declaring the company has more than 50 workers (34.6%), followed by '5-20 employees' (30.80%), '1-5 employees' (18%), and lastly, '21-50 employees' (16.50%). The distribution of working experience met the logical expectation of this study. Since the respondents have been working in the same company for several years, they would have the experience and knowledge of the company's existing working culture, internal control, and information technology systems. The respondents' work experience implied that they have their own perception of the influence of fraud prevention mechanisms on occupational fraud.

Table 3: Demographic Profile of Respondents

Description		Total	
		N = 133	Percentage (%)
Gender	Male	67	50.40
	Female	66	49.60
Age	18-29 years old	14	10.50

	30-39 years old	68	51.10
	40-49 years old	25	18.80
	50-59 years old	22	16.50
	Above 60 years old	4	3.00
Marital status	Single	31	23.30
	Married	100	75.20
	Divorced/Widowed/ Separated	2	1.50
Highest education level	SPM/STAM	7	5.30
	Diploma	18	13.50
	Bachelor /Degree	77	57.90
	Professional	9	6.80
	Master/PHD	22	16.50
Position in the organisation	Business Owner/Director	55	41.40
	Executive/Clerks	78	58.60
Type of business entity	Sole Proprietorship	15	11.30
	Partnership	12	9.00
	Limited Liability Partnership	5	3.80
	Private Limited Company	86	64.70
	Professional, i.e., Solicitor, Accountant, Surveyor	15	11.30
Nature of business	Food & Beverages /Restaurant	7	5.30
	IT / Network	8	6.00
	Manufacturing	10	7.50
	Others	31	23.30
	Plantation / Agriculture /Farming	4	3.00
	Professional Services (Doctor, Surveyor, Auditor, Solicitor)	22	16.50
	Retailer / Wholesaler	18	13.50
	Services	33	24.80
Estimated number of employees in the organisation	1-4 employees	24	18.00
	5-20 employees	41	30.80
	21-50 employees	22	16.50
	More than 50 employees	46	34.60
Number of years working in this organisation	Less than 1 year	1	0.80
	1-5 years	47	35.30
	6-10 years	44	33.10
	11-20 years	24	18.00
	More than 20 years	17	12.80

Descriptive Analysis

Occupational Fraud

Table 4 presents the results of the descriptive analysis of occupational fraud based on the employees' perspective. The measuring items given covered all three types of occupational fraud and the abuse classification system under The Fraud Tree: Corruption, Asset Misappropriation, and Financial Statement Fraud. The 5-point Likert scale used was '1' (Strongly Disagree), '2' (Disagree), '3' (Slightly Agree), '4' (Agree), and '5' (Strongly Agree). The mean scores were sorted in descending order to determine the respondents' level of agreement with the items. The mean for all items is between 2.56 and 1.35. These values indicate that almost all respondents disagree with the occurrence of each occupational fraud type in their organisations. The highest mean score (2.56) is for the statement 'You have experienced/witnessed fraud activities in your organisation'. The statement 'It is acceptable to take gifts from clients instead of receiving money' also has a high mean score of 2.38, implying that many employees disagree with the statement. The lowest mean (1.35) is for 'Creating fraudulent electronic documents and files are acceptable since they can easily be erased/deleted'. In other words, many employees strongly disagree with creating fraudulent electronic documents despite their erasability. The mean scores, ranging from 1.0 to 1.74, indicate a high level of awareness among respondents regarding occupational fraud. They strongly disagree with scenarios involving falsifying documents, forging signatures, skimming, and overstating personal claims. However, they only slightly disagree with scenarios related to accepting gifts and misusing the company's assets for personal consumption.

Table 4: Descriptive Statistics for Employees' Perception of Occupational Fraud

Statement	Mean	Std. Deviation
You have experienced /witnessed fraud activities in your organisation.	2.56	1.362
It is acceptable to take gifts from clients instead of receiving money.	2.38	1.417
It is acceptable to take some of the company's assets, such as stationery, for personal use at home.	2.00	1.291
Alteration of financial statements is acceptable to show better company performance.	1.74	1.193
Colluding with a contractor by increasing the quotation value when entering a contract is acceptable.	1.66	1.141
Signature forgery on the company's document is deemed acceptable in a state of emergency.	1.49	1.005
It is acceptable to falsify financial statements to request bank loans.	1.46	1.011
When requesting reimbursement of business expenses, it is acceptable to make higher claims than what it is supposed to be.	1.40	0.825
Revealing the company's confidential information to a third party who is found to be a competitor is deemed appropriate.	1.39	0.96

Entering lower cash sales as 'cash received from customer' in the sales register is deemed acceptable when you are facing financial distress and in need of money.	1.38	0.926
Creating fraudulent electronic documents and files is acceptable since they can easily be erased/deleted.	1.35	0.828
N = 133		

Ethical Culture

Table 5 tabulates the descriptive analysis of the employees' perspective on ethical culture. The mean scores are sorted in descending order to determine the respondents' level of agreement with the statements. The means for all statements are between 4.56 to 3.83. These values indicate that almost all respondents agree that an ethical culture would refrain from occupational fraud in the organisation. The highest mean (4.56) is for 'A good ethical culture will prevent the company from being involved in fraud activities.' In other words, many employees agree that a good ethical culture can be a fraud prevention mechanism. The lowest mean (3.83) is for 'The management has made known to you Section 17A of the Malaysian Anti-Corruption Commission Act (MACC Act), which stipulates a corporate liability principle, where a commercial organisation can be considered guilty if any of its employees and/or associates commit corruption for the benefits of the organisation.' This mean score indicates that many employees think that the management might have informed them of this provision of the MACC Act. When asked about the effectiveness of ethical culture in preventing fraud, the employees perceived that having a good ethical culture is effective in refraining them from being involved in any fraud activities when dealing with third parties (mean score = 4.50). They also perceived that the management's practice of a good ethical culture is effective in curbing fraud activities in their organisations (mean score = 4.36). Hence, both statements suggest that a strong ethical culture can refrain employees from committing fraud with minimal supervision. This has been acknowledged through the mean score of 3.89 for the statement of "During the COVID19 pandemic, how effective is good ethical culture in refraining employees from committing fraud activities, especially when they are working from home?", which indicates that despite working remotely, the integrity of an individual and good ethical culture can curb fraud activities from occurring.

Table 5: Descriptive Statistics for Employees' Perception of Ethical Culture

Statement/Question	Mean	Std. Deviation
A good ethical culture will prevent the company from being involved in fraud activities.	4.56	0.908
In your opinion, how effective is having a good ethical culture in refraining employees from being involved in any fraud activities, especially when dealing with suppliers/customers outside of the organisation for business?	4.50	0.804
The management team promotes tone-at-the-top culture of honesty and integrity in the organisation.	4.47	0.875

In your opinion, how effective is the management's practice of good ethical culture in the company? These include effective two-way communication between employees and the management team, encouraging employees to communicate any wrongdoings of their colleagues, and emphasis on avoiding bribery/embezzlement of the company's money.	4.36	0.856
The management team has a zero-tolerance policy of employees committing fraud and has emphasised it in meetings/actions/words.	4.16	0.999
You know how to seek opinions/advice when faced with difficult/uncertain ethical decisions.	4.06	1.013
Your company implements a 'Code of Conduct' for all levels of employees that clearly defines actions that are permitted and prohibited in your company.	4.04	1.018
Your company is using an ethical culture to reduce fraud incidents effectively.	3.96	1.018
Your management promotes a 'Speak-Up Culture' for all known and potential wrongdoings occurring in the organisation.	3.91	1.138
During the COVID19 pandemic, how effective is a good ethical culture in refraining employees from committing fraud activities, especially when they are working from home?	3.89	1.116
The management has made known to you Section 17A of the Malaysian Anti-Corruption Commission Act (MACC Act), which stipulates a corporate liability principle where a commercial organisation can be considered guilty if any of its employees and/or associates commit corruption for the benefit of the organisation.	3.83	1.346
N = 133		

Internal Control

Table 6 displays the descriptive analysis of the employees' perspective on internal control. The mean scores are sorted from highest to lowest values. The means for all statements and questions are between 4.20 and 2.81. This range indicates that the respondents disagree with some of the items measuring internal control as a mechanism to prevent occupational fraud in the organisation. The highest mean (4.20) is for 'Your company has proper approval limits that relate to banking transactions/cheque signatories.' This score implies that most companies implement an internal control mechanism for banking transactions. The lowest mean (2.81) is for 'You have attended anti-fraud programmes, whether organised in-house or by third parties.' The low mean score suggests that many employees disagree with this statement. It could be that many employees were not given specific training on the use of internal control to curb occupational fraud, or the companies lack resources for employees to attend anti-fraud programmes. This outcome helps explain why the degree of awareness of internal control as a fraud prevention mechanism is still at a moderate level. Regarding the effectiveness of internal control as a fraud prevention mechanism, most employees perceived that segregation of duties is either effective or slightly effective in preventing fraud (mean score = 3.78). They have similar perceptions of the effectiveness of internal control in mitigating fraud risks in the

organisation (mean score 3.60). Table 6 also shows that internal control is less effective during the Covid19 pandemic (mean score 3.28), probably because it is difficult to monitor the employees who are working from home.

Table 6: Descriptive Statistics for Employees' Perception of Internal Control

Statements	Mean	Std. Deviation
Your company has proper approval limits that relate to banking transactions/cheque signatories.	4.20	1.17
How would you rate the effectiveness of the segregation of duties in your organisation?	3.78	1.00
Your company has proper authorisation for assessing confidential documents.	3.74	1.17
Your company has an effective hiring process, such as criminal and civil background checks, reference checks, drug screening, and education validation.	3.66	1.24
How would you rate the effectiveness of your company's internal control in reducing fraud risk in the organisation?	3.60	0.98
Your company has a policy of mandatory holidays every year.	3.52	1.41
Your company develops policies for workstation use, such as access restrictions and clear-desk policy. Clear-desk policy is to ensure that the workstation is clean by the end of the day, and all confidential information/documents have been kept properly and are not lying on the table.	3.48	1.29
Your company implements a logging system that logs all activities performed by employees that would be useful to detect any unauthorised access.	3.38	1.39
During the COVID19 pandemic, how would you rate the effectiveness of the company's internal control in curbing fraud activities, as most employees are working from home and no physical monitoring can be done?	3.28	1.02
Your company conducts fraud risk assessments.	3.17	1.25
You have attended anti-fraud programmes, whether organised in-house or by third parties.	2.81	1.51
N = 133		

Information Technology Systems

Table 7 presents the descriptive analysis of information technology systems from the employees' perspective. The mean scores are sorted from highest to lowest value to determine the level of the respondents' perception of this variable. The mean scores for all items are between 4.66 and 3.31. The means indicate that almost all respondents agree that information technology systems would prevent occupational fraud in the organisation. The highest mean of 4.66 shows that the employees believe that cybercrime has increased over the years. However, despite this increase, their companies still use e-banking services for almost all business

transactions. This usage is probably because of the convenience of e-banking. The lowest mean of 3.31 indicates that employees slightly agree that their companies allow them to access any websites and download any applications from the internet, implying that some employees have restricted access to certain websites. Regarding the effectiveness of the IT system, most employees believe that the use of appropriate accounting software to record all financial activities is effective in reducing fraud attempts (mean score = 4.23). However, they think that the IT system is only slightly effective in reducing fraud activities (mean score = 3.91) and fraud risks (mean score = 3.95) in their organisations.

Table 7: Descriptive Statistics for Employees' Perception of Information Technology Systems

Statements	Mean	Std. Deviation
Cybercrime has increased over the years.	4.66	0.602
Your company uses e-banking services for almost all business transactions, such as paying suppliers, staff salaries, and overhead expenses.	4.38	0.911
In your opinion, how effective is your company's use of appropriate accounting software to record all financial activities in reducing fraud attempts?	4.23	0.887
Your company installs firewall protection and anti-virus protection in all the computers/notebooks.	4.18	1.079
Your company ensures that the firewall protection and anti-virus protection are updated on a regular basis.	4.16	1.006
In your opinion, how would you rate the effectiveness of your company in using information technology system to reduce fraud risks in the organisation?	3.95	0.895
In your opinion, how effective is technology, such as business application software, internet, and e-banking, in reducing fraud activities in the organisation?	3.91	0.965
Your company has unique identifiers to define each user's identity in electronic records, e.g., username.	3.50	1.428
Your company blocks certain websites to be accessed by the employees to refrain from being hacked by fraud perpetrator / outsiders.	3.41	1.404
Your company has auto log-off or session termination after specified time of inactivity, especially to protect confidential information in your organisation.	3.37	1.427
Your company allows access to any websites and to download any application from the internet.	3.31	1.431
<i>N</i> = 133		

Reliability Analysis

As shown in Table 8, the Cronbach's alpha coefficient for this study is 0.878 for the perception of occupational fraud, followed by 0.863 for the perception of ethical culture, 0.839 for the perception of internal control, and 0.713 for the perception of information technology system. Hence, all the variables' Cronbach's alpha coefficients exceed the desired threshold of 0.7, indicating an acceptable degree of internal consistency.

Table 8: Summary of Reliability Test Using Cronbach's Alpha

Variable	Cronbach's Alpha	N of Items
Occupational Fraud (DV)	0.878	11
Ethical Culture (IV)	0.863	11
Internal Control (IV)	0.839	11
Information Technology Systems (IV)	0.713	11

Normality Analysis

A normality test was conducted to determine whether the data were normally distributed (refer to Table 9). The analysis was performed using skewness and kurtosis values for occupational fraud, ethical culture, internal control, and information technology system. According to George and Mallery (2021), values for skewness and kurtosis in the range of -2 to +2 are acceptable for the data to be considered normally distributed. Hair et al. (2010) argued that data distribution is normal if the skewness is between -2 and +2 and the kurtosis ranges from -7 to +7. For this study, Table 9 shows that the skewness ranges from -2 to +2 and the kurtosis ranges from -7 to +7 for all factors. Therefore, the data for all the predictors are normally distributed.

Table 9: Summary of Skewness and Kurtosis

Variable	Skewness		Kurtosis	
	Statistic	Std. Error	Statistic	Std. Error
Occupational Fraud	1.859	0.21	4.26	0.417
Ethical Culture	-0.554	0.21	-0.435	0.417
Internal Control	-0.012	0.21	-0.057	0.417
Information Technology Systems	-0.332	0.21	-0.095	0.417

$N = 133$

Correlation Analysis

Table 10 indicates a weak, inverse correlation between ethical culture and occupational fraud ($r = -0.271$). It suggests that a strong ethical culture will reduce the occurrence of occupational fraud in an organisation. The relationship is significant at the 99% level of confidence ($p = 0.01$). The next factor is internal control. Tables 10 and 11 show a weak, negative correlation

between the two variables ($r = -0.177$). However, although weak, the relationship is significant at the 0.05 level. Another variable is IT systems. Table 10 also shows a weak, negative correlation between IT systems and occupational fraud ($r = -0.17$). However, the relationship is not significant.

Table 10: Correlation Summary

Variables	OC	EC	IC	ITS
Occupational Fraud (OC)	1			
Ethical Culture (EC)	-0.271**	1		
Internal Control (IC)	-0.177*	0.606**	1	
Information Technology Systems (ITS)	-0.170	0.473**	0.601**	1

** . Correlation is significant at the 0.01 level (2-tailed).

* . Correlation is significant at the 0.05 level (2-tailed).

$N = 133$

Multicollinearity Test

Table 11 shows that all the tolerance values of the independent variables are greater than 0.1 (Pallant, 2020) and 0.2 (Hair et al., 2010). Meanwhile, their VIF values are below 10. Thus, it can be concluded that the independent variables have no multicollinearity issues and are suitable for multiple regression analysis.

Table 11: Summary of Collinearity Analysis

Model	Collinearity	
	Tolerance	VIF
Ethical Culture	0.614	1.629
Internal Control	0.505	1.979
Information Technology Systems	0.620	1.614

Dependent Variable: Occupational Fraud

Multiple Regression Analysis

Table 12 reveals the results of the multiple regression analysis of this study. The F-change value ($F = 3.513$, $p\text{-value} < 0.05$) indicates that the model used in this study is statistically significant. Further, the R^2 value ($R^2 = 0.275$) indicates that the model is fit and acceptable. Hair et al. (2010) asserted that a model with an R-squared value greater than 0.10 is considered fit. The result also implies that the independent variables (ethical culture, internal control, and IT systems) collectively explain 27.5% of the variation of the dependent variable (occupational fraud). As shown in Table 13, only the employees' perception of ethical culture is significant to occupational fraud, as its p-value is less than 0.05. The two (2) independent variables are not significant to the dependent variable since their p-values are greater than 0.05. The table also shows a negative significant linear relationship between ethical culture and occupational fraud in SMEs ($t(95) = -2.299$, $p = 0.023$). Further, the results show an insignificant positive linear relationship between internal control and occupational fraud in SMEs ($t(95) = 0.069$, $p =$

0.945). Similarly, IT systems have an insignificant negative linear relationship with occupational fraud in SMEs ($t(95) = -0.534$, $p = 0.594$). However, since the p-value is less than 0.10, the relationship could still be considered relevant at the 90% confidence level.

Table 12 also presents the standardised beta coefficient (b) of each independent variable in the model. The value for ethical culture ($b = -0.248$) indicates that when the effectiveness of ethical culture increases by one unit, the possibility of occupational fraud will decrease by 0.248 units. This interpretation is true only if the effects of internal control and IT systems are held constant. The beta value for internal control ($b = 0.008$) indicates that when its effectiveness increases by one unit, the possibility of occupational fraud will increase by 0.008 units. This interpretation is true only if the effects of ethical culture and IT systems are held constant. IT systems have a beta value of -0.057, indicating that when its effectiveness increases by one-unit, occupational fraud will decrease by 0.057 units. This interpretation is true only if the effects of ethical culture and internal control are held constant.

Table 12: Multiple Regressions Between Fraud Prevention Mechanisms and Occupational Fraud

Model	B	Std. Error	Beta (b)	t	Sig.
(Constant)	34.408	5.379		6.396	0
Ethical Culture	-0.278	0.121	-0.248	-2.299	0.023*
Internal Control	0.008	0.116	0.008	0.069	0.945
Information Technology Systems	-0.074	0.139	-0.057	-0.534	0.594
R ²					0.275
Adjusted R ²					0.076
F Change					3.513*

Dependent Variable: Occupational Fraud

*p-value = 0.17

Conclusion

This study showed that employees still believe in information technology systems as one of the useful fraud prevention mechanisms. Despite the increasing digital fraud risk due to a sophisticated business environment, employees still view IT systems as effective in curbing fraud activities. However, technological advancement cannot be controlled by manual processes. Therefore, SMEs must be aware of new changes in technology that are within their financial budget and expertise to protect the companies' interests. This study did not support the second hypothesis on the significant negative relationship between internal controls and occupational fraud in SMEs. Based on the employees' perceptions, good personality traits need to be instilled to combat the evil intention to commit fraud rather than other means of internal control. Hence, they prefer setting an ethical culture as a priority over internal control in preventing occupational fraud. This is because the respondents hold different positions in the company, and the business owners/directors are the ones who need to set the right ethical culture on top of establishing internal control in the organisation. In a nutshell, ethical culture is a major factor in providing the right control environment for people operating within

organisations. It is the major defence mechanism in preventing fraud. Hence, it is suggested to have the right culture embedded in the company, such as a highly motivated workforce, excellent morale, staff with high integrity, the ability to understand and take responsibility, and the ability to manage change. The last attribute is especially important for effective and efficient information technology systems. By having these effective fraud prevention mechanisms, SMEs would curb the elements in the Fraud Hexagon theory, namely stimulus/incentive, capability, opportunity, rationalisation, ego, and collusion.

The study has practical implications for SME business owners. The findings indicate that ethical culture is of the utmost value to be upheld when dealing with internal and external parties. Thus, it is the duty of management and business owners to lead by good example and take responsibility for effective communication and actions to cultivate a good working environment to prevent fraud. While the importance of ethical culture in fraud prevention is not new, this study provides original insights specific to the context of Malaysian SMEs. These insights could enrich the existing literature and offer a unique perspective on fraud prevention in SMEs. Since SMEs have no regulators, such as Security Commissions, this study can provide basic information for SME Corp to ensure proper handbooks, training, and awareness programmes on managing their company and reducing fraud risk are available to SME owners. The findings provide an uncommon account to SMEs in a developing country, such as Malaysia, on the importance of ethical culture, information technology systems, and monitoring activities in preventing occupational fraud. The implication for the accounting profession is to ensure that accounting firms educate and advise their clients on how crucial it is to have a proper fraud prevention mechanism to minimise and deter fraud. For larger companies regulated by the Security Commission, it is notable that they are also governed by the Malaysian Code of Corporate Governance (MCCG), which highlights the importance of corporate governance to prevent unwanted conflicts. Among the pillars emphasised in the MCCG are ethical behaviour, accountability, transparency, and sustainability, which are essential to companies' governance and to produce long-term value (MCCG, 2021). The pillars further prove that ethical value is deemed the most important part of internal control, processes, and procedures to deter occupational fraud. Additionally, the findings of this study may provide practical insights that are directly relevant to SME business owners. By emphasising the importance of ethical culture and the role of management and business owners in setting the tone, this study offers actionable recommendations for preventing fraud. This practical relevance makes the research valuable to a wide audience of SME practitioners.

There are a few limitations of this study. Firstly, the duration of the study was five (5) months, from research design to data analysis. Secondly, the sample size is 133, and the respondents are located in the Klang Valley. The research period, sample size, and company locations could be expanded in future research. Thirdly, the variables selected in the study were ethical culture, internal control, and information technology systems. Future research could expand the selection of variables to examine the effectiveness of fraud prevention tools. Extensions to the present study are possible in the following areas. First, future research could explore the use of fraud prevention mechanisms in different states in Malaysia since this study focused only on the Klang Valley. Further, a comparison of the fraud prevention mechanisms between large corporations and SMEs could be explored to determine which fraud prevention mechanism is cost-effective and beneficial for SMEs. Second, due to limited resources, especially financial resources, SMEs are reluctant to engage forensic accountants when fraud occurs. Therefore, future studies could look at a sample of companies that hired forensic accountants to investigate fraud in their premises and study the effectiveness of the existing fraud prevention mechanisms.

-
- Acknowledgements:** The authors would like to express their sincere gratitude to University Teknologi MARA, Cawangan Selangor, Kampus Puncak Alam for providing the necessary resources and support throughout the course of this research. Special appreciation is extended to colleagues and peers who contributed valuable insights and constructive feedback, which greatly enhanced the quality of this paper.
- Funding Statement:** No Funding
- Conflict of Interest Statement:** The authors declare that there is no conflict of interest regarding the publication of this paper. All authors have contributed to this work and approved the final version of the manuscript for submission to the Advanced International Journal of Business, Entrepreneurship and SMEs (AIJBES).
- Ethics Statement:** This study was conducted in accordance with ethical research standards. All procedures involving human participants were reviewed and approved by the UiTM Research Ethics Committee, approval number REC/08/2021 (MR/639). Informed consent was obtained from all participants prior to data collection. Participation was voluntary, and respondents were assured of confidentiality and anonymity. The data collected were used solely for academic purposes.
- Author Contribution Statement:** All authors contributed significantly to the development of this manuscript. Nadiah H. Saharuddin handled literature review, data collection, analysis, and interpretation of results. Mazurina Mohd Ali was responsible for the conceptualisation, methodology and overall supervision of the study. Mazurina Mohd Ali and Noor Hasniza Haron contributed to the critical revision of the manuscript. Suhaily Hasnan contributed to the drafting and analysis. All authors read and approved the final version of the manuscript prior to submission.
-

References

- Agarwal, R., & Kallapur, S. (2018). Cognitive risk culture and advanced roles of actors in risk governance: A case study. *The Journal of Risk Finance*, 19(4), 327-342.
- Ali, M. M., Ayop, N. F., Ghani, E. K., & Hasnan, S. (2020). The effect of employees' perceptions on internal control system mechanisms towards employee fraud prevention. *Journal of Critical Reviews*, 7(18), 972-986.
- Ali, M. M., Ghani, E. K., Muhammad, K., & Widuri, R. (2023). Accounting service quality by small and medium practices: A review. *Journal Corporate and Business Strategy Review*, 4(2), 270-279.
- Arens, A. A., Elder, R. J., & Beasley, M. S. (2017). *Auditing and assurance services: An integrated approach*. Pearson.
- Association of Certified Fraud Examiners (ACFE) (2022). A report to the nations. *ACFE: <https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf>*, 8, 2023.
- Barlaup, K., Iren Drønen, H., & Stuart, I. (2009). Restoring trust in auditing: Ethical discernment and the Adelphia scandal. *Managerial Auditing Journal*, 24(2), 183-203.
- Bishop, T. J. (2004). Preventing, deterring, and detecting fraud: What works and what doesn't. *Journal of Investment Compliance*, 5(2), 120-127.
- Chalmers, K., Hay, D., & Khelif, H. (2019). Internal control in accounting research: A review. *Journal of Accounting Literature*, 42(1), 80-103.
- COSO (2019). *COSO internal control – Integrated framework*. Available at: www.Coso.Org/Documents/COSO-CROWE-COSO-Internal-Control-Integrated-Framework.Pdf
- Cressey, D. R. (1953). *Other people's money; A study of the social psychology of embezzlement*. Free Press.
- Dorminey, J., Fleming, A. S., Kranacher, M. J., & Riley Jr, R. A. (2012). The evolution of fraud theory. *Issues in Accounting Education*, 27(2), 555-579.
- Eltayeb, T. K., Zailani, S., & Ramayah, T. (2011). Green supply chain initiatives among certified companies in Malaysia and environmental sustainability: Investigating the outcomes. *Resources, Conservation, and Recycling*, 55(5), 495-506.
- George, D., & Mallery, P. (2021). *IBM SPSS statistics 27 step by step: A simple guide and reference*. Routledge.
- Gunasegaran, M., Basiruddin, R., Abdul Rasid, S. Z., & Mohd Rizal, A. (2018). The case studies of fraud prevention mechanisms in the Malaysian medium enterprises. *Journal of Financial Crime*, 25(4), 1024-1038.
- Hair, J. F., Anderson, R. E., Babin, B. J., & Black, W. C. (2010). *Multivariate data analysis: A global perspective* (Vol. 7).
- Halbouni, S. S., Obeid, N., & Garbou, A. (2016). Corporate governance and information technology in fraud prevention and detection: Evidence from the UAE. *Managerial Auditing Journal*, 31(6/7), 589-628.
- Khan, M. (2006). Determinants of corruption in developing countries: The limits of conventional economic analysis. *International Handbook on the Economics of Corruption*, 216-244.
- Krambia-Kapardis, M., & Zopiatis, A. (2010). Investigating incidents of fraud in small economies: The case for Cyprus. *Journal of Financial Crime*, 17(2), 195-209.
- Kramer, B. (2015). Trust, but verify: Fraud in small businesses. *Journal of Small Business and Enterprise Development*, 22(1), 4-20.

- Le, N. T., Vu, L. T., & Nguyen, T. V. (2021). The use of internal control systems and codes of conduct as anti-corruption practices: Evidence from Vietnamese firms. *Baltic Journal of Management*, 16(2), 173-189.
- Murphy, P. R., & Dacin, M. T. (2011). Psychological pathways to fraud: Understanding and preventing fraud in organisations. *Journal of Business Ethics*, 101, 601-618.
- Nawawi, A., & Salin, A. S. A. P. (2018). Internal control and employees' occupational fraud on expenditure claims. *Journal of Financial Crime*, 25(3), 891-906.
- Nguyen, T. V., Ho, B. D., Le, C. Q., & Nguyen, H. V. (2016). Strategic and transactional costs of corruption: Perspectives from Vietnamese firms. *Crime, Law, and Social Change*, 65, 351-374.
- Omar, N., & Abu Bakar, K. M. (2012). Fraud prevention mechanisms of Malaysian government-linked companies: An assessment of existence and effectiveness. *Journal of Modern Accounting and Auditing*, 8(1), 15-31.
- Omar, M., Nawawi, A., & Puteh Salin, A. S. A. (2016). The causes, impact, and prevention of employee fraud: A case study of an automotive company. *Journal of Financial Crime*, 23(4), 1012-1027.
- Pallant, J. (2020). *SPSS survival manual: A step-by-step guide to data analysis using IBM SPSS*. McGraw-Hill Education.
- Peltier-Rivest, D., & Lanoue, N. (2011). Thieves from within: Occupational fraud in Canada. *Journal of Financial Crime*, 19(1), 54-64.
- Parthiban, P., Goswami, N., Radhika, S. N. J., Choudari, S., & Shokeen, A. (2026). Ethical leadership and its influence on workplace integrity and employee accountability. *Journal of Daoist Studies*, 19(S4), 983-996.
- Power, M. (2013). The apparatus of fraud risk. *Accounting, Organizations, and Society*, 38(6-7), 525-543.
- Rahman, N. H. A., Jamaluddin, A., Hamzah, N., & Aziz, K. A. (2019). Establishing an effective internal control system for fraud prevention: A structured literature review. *Asia-Pacific Management Accounting Journal*, 14(3), 21-47.
- Rashid, M. A., Al-Mamun, A., Roudaki, H., & Yasser, Q. R. (2022). An overview of corporate fraud and its prevention approach. *Australasian Accounting, Business, and Finance Journal*, 16(1).
- Sekaran, U. & Bougie, R. (2016). *Research methods for business: A skill-building approach*. John Wiley & Sons.
- Sengur, E. D. (2012). Auditors' perception of fraud prevention measures: Evidence from Turkey. *Annales Universitatis Apulensis: Series Oeconomica*, 14(1), 128.
- Sow, A. N. G., Basiruddin, R., Abdul Rasid, S. Z., & Husin, M. M. (2018a). Understanding fraud in Malaysian SMEs. *Journal of Financial Crime*, 25(3), 870-881.
- Sow, A. N. G., Basiruddin, R., Mohammad, J., & Rasid, S. Z. A. (2018b). Fraud prevention in Malaysian small and medium enterprises (SMEs). *Journal of Financial Crime*, 25(2), 499-517.
- Suryanto, T. (2016). Dividend policy, information technology, accounting reporting to investor reaction and fraud prevention. *International Journal of Economic Perspectives*, 10(1).
- Vousinas, G. L. (2019). Advancing theory of fraud: The SCORE model. *Journal of Financial Crime*, 26(1), 372-381.
- Wells, J. T. (2017). *Corporate fraud handbook: Prevention and detection*. John Wiley & Sons.
- Zainal, S. F., Hashim, H. A., Ariff, A. M., & Salleh, Z. (2022). Research on fraud: An overview from small and medium enterprises (SMEs). *Journal of Financial Crime*, 29(4), 1283-1296.

Zakaria, K. M., Nawawi, A., & Salin, A. S. A. P. (2016). Internal controls and fraud: Empirical evidence from an oil and gas company. *Journal of Financial Crime*, 23(4), 1154-1168.