

Fraud Prevention in Flux: Are Traditional Methods Holding Their Ground in the Digital Age? Evidence From an Emerging Economy

Kaushalya Silva* and Roshan Ajward

ABSTRACT

Manuscript type: Research paper

Research aims: This study investigates the perceived level of fraud occurrence and the utilisation of traditional and technological fraud deterrence tools in listed companies (LCs) in Sri Lanka, while exploring differences in such perceptions between LC employees and external auditors, given the limited empirical evidence in emerging economies.

Design/Methodology/Approach: Guided by a postpositivist paradigm, a self-administered structured survey was conducted targeting top-level and middle-management-level employees in LCs and external auditors in Sri Lanka using a random sample. A total of 229 usable responses, including 127 LC employees and 102 external auditors, were analysed using non-parametric statistical techniques.

Research findings: Findings confirm the prevalence of fraud in LCs, acknowledged by both LC employees and external auditors, with no significant perceptual differences. Both respondent groups perceive traditional tools to be more widely utilised than technological tools in deterring fraud in LCs. However, in terms of perceptual differences, LC employees perceive a higher usage of traditional tools than external auditors, while no significant difference exists in technological tools usage. Widely utilised traditional tools include bank reconciliations, internal

* Corresponding Author. Kaushalya Silva is a Senior Lecturer at the Department of Accountancy, Faculty of Commerce and Management Studies, University of Kelaniya, Sri Lanka. Her research interests include corporate governance, capital markets, micro and macroeconomic environment, and corporate fraud. Email: kaushalyas@kln.ac.lk
Roshan Ajward is a Professor in Accounting attached to the Department of Accounting, University of Sri Jayewardenepura, Sri Lanka. His research interests include the impact of corporate governance mechanisms on financial accounting dimensions, such as earnings quality, and contemporary issues in auditing and assurance services. Email: ajward@sjp.ac.lk

audits, and inventory observations, whereas forensic accountants, fraud departments and whistleblowing policies were among the least utilised traditional tools. Basic technological tools like password protection, firewalls, and virus protection were commonly utilised, whereas advanced technological tools like Bayesian networks, Benford's Law, neural networks and digital forensic tools were rarely utilised, signalling a significant technological lag in addressing the complex nature of modern fraud.

Originality: As a pioneering empirical study in an emerging economy context, this study offers new insights into a wide array of traditional and technological fraud deterrence techniques through a comparative professional lens, particularly amid regional governance challenges. The study contributes to the fraud deterrence literature by providing empirical insights into fraud deterrence practices in an emerging economy, highlighting the growing importance of technology-driven techniques for real-time fraud deterrence, despite continued reliance on traditional mechanisms. Moreover, the findings offer policymakers practical guidance for strengthening fraud deterrence and enhancing transparency in financial reporting through the lenses of Cognitive Dissonance and Social Identity theories.

Keywords: Emerging Economies, Fraud, Fraud Prevention and Detection, Listed Companies, Technological Tools, Traditional Tools

JEL Classification: M42, K42, G34, O33, O16

1. Introduction

In today's fast-moving and highly dynamic business environment, led by rapid technological advancements, fraud has become a global dilemma affecting all organisations worldwide (ACFE, 2024; Ernst & Young, 2018). The Association of Certified Fraud Examiners, in its *Occupational Fraud 2024: A Report to the Nations*, emphasises that fraud across 138 countries and territories has resulted in total losses of more than USD 3.1 billion between January 2022 and September 2023 (ACFE, 2024). They further emphasise that, on average, a fraud case goes undetected for 12 months, causing a median loss of USD 145,000 per case. Compounding these realities, the high-profile bankruptcies such as Enron and WorldCom have significantly diminished stakeholders' trust in global financial markets and the accounting profession (Law, 2011). Beyond financial losses, fraud undermines organisation's ability to provide employment and quality products and services (ACFE, 2020). Moreover, the digital transformation era has led organisations to extensively rely on technology, increasing their vulnerability to fraud and other risks (Alleyne & Howard, 2005). Existing literature in the Asian context highlights that rapid

technological disruption necessitates the accounting profession to evolve its skill set to maintain audit quality and deter fraud in digital environments (Indrayani et al., 2025). Thus, organisations must estimate the extent of fraud and its associated costs since not all fraud is detected or reported (Farrell & Franco, 1999; In'airat, 2015).

Ernst and Young (2018) emphasise that weak governance and ineffective fraud prevention mechanisms have collectively fueled the rise in organisational fraud. Mangala and Kumari (2017) highlight that combating fraud requires the implementation of preventive measures and continuous monitoring. Hence, it is imperative to give proper attention to prevention and detection techniques, swiftly followed by stringent actions upon uncovering fraudulent activities. Rahman and Anwar (2014) emphasise that both prevention and detection methods should be implemented concurrently in organisations to successfully combat pervasive fraud. Peiris and Aruppala (2021) state that fraud is rising due to higher potential gains and lower detection risk, highlighting the need for advanced fraud prevention and detection mechanisms by organisations and governing authorities. The integration of artificial intelligence and other technological advancements has significantly enhanced real-time fraud prevention and detection across various sectors (Ali et al., 2024; Rao et al., 2025). Thus, given the pervasive nature of fraud, both traditional and technological fraud prevention and detection techniques are crucial in deterring fraud, improving organisational performance and, thereby, safeguarding its well-being.

Accordingly, this study aims to assess the perceptions of listed company employees and external auditors in Sri Lanka, an emerging economy, regarding fraud occurrence and the usage of traditional and technological fraud prevention and detection techniques, while also examining differences in such perceptions between the two respondent groups. Focusing on emerging economies is particularly important due to the high vulnerability of such organisations to fraud. ACFE (2024) reveals that Southern Asia reported the highest number of fraud cases accounting for 74% of the 1,921 cases examined across eight regions, while Ernst and Young (2018) emphasise that fraud remains more prevalent in emerging markets due to weaker institutional and governance structures. In the Sri Lankan context, the pervasive presence of corruption and corporate misconduct remains a critical challenge, adversely affecting organisational performance and investor confidence (Ramesh & Vinayagathan, 2024). Several high-profile financial scandals, including the Golden Key Credit Card Company, The Finance Company PLC, ETI Finance Ltd., and

Swarnamahal Financial Services PLC, continue to serve as significant reminders of the consequences of governance deficiencies and weak regulatory oversight (Rathnasiri & Bandara, 2017; Dissanayake et al., 2022). The persistent nature of this issue is further evidenced by recent regulatory interventions, such as the cancellation of Bimpuh Finance PLC's license in 2023 and the ongoing state-managed resolution of Nation Lanka Finance PLC, which has been extended through mid-2026 (Central Bank of Sri Lanka [CBSL], 2023, 2026). Furthermore, the rise of sophisticated digital-age frauds, notably the prohibited pyramid schemes including OnmaxDT and MTFE, that resulted in massive public losses in 2024 and 2025, emphasise the immediate need for robust fraud deterrence mechanisms (CBSL, 2025). Strengthening these mechanisms, reinforced by the enactment of the Anti-Corruption Act, No. 9 of 2023, remains a national priority for ensuring transparency and integrity in the corporate sector (CBSL, 2024). Despite the growing prevalence of complex corporate fraud, prior studies have largely focused on developed countries (Grove & Basilico, 2008; Ngai et al., 2011), with relatively few empirical studies investigating this phenomenon in emerging contexts (Halbouni et al., 2016). Therefore, this study addresses the dearth of empirical research on fraud prevention and detection in emerging economies, a gap further intensified by the mixed evidence from prior studies. While previous studies have examined individual fraud prevention and detection techniques or focused on specific professional groups, there is a dearth of studies exploring the simultaneous deployment of both traditional and technological fraud deterrence mechanisms, as well as comparing perceptions between internal organisational members and external auditors in emerging contexts. By addressing this empirical gap, the present study provides new empirical insights into fraud deterrence practices in Sri Lankan listed companies.

Additionally, this study pioneers the use of a robust multi-theoretical lens to investigate an expanded suite of 27 traditional and 31 emerging technological fraud deterrence tools. Unlike previous studies that rely solely on the traditional fraud triangle and fraud diamond, this study incorporates the fraud hexagon and organisational fraud triangle to provide a nuanced understanding of how *leadership*, *culture*, and *complex behaviours* like *collusion* influence fraud deterrence in an emerging economy. Furthermore, by integrating Social Identity Theory and Cognitive Dissonance Theory, this study provides a robust theoretical justification for the divergent perceptions observed between LC employees and external auditors regarding the usage of traditional and technological fraud deterrence

tools. By doing so, these theoretical frameworks serve as lenses for explaining how professional identity and the need for cognitive consistency shape the way that different cohorts perceive and value traditional versus technological fraud deterrence mechanisms in the digital age.

The rest of this paper is structured as follows: Section 2 provides a comprehensive review of the literature and formulates the research hypotheses. Section 3 delineates the research methodology, including data collection and analysis strategies, while Section 4 presents empirical findings and discussion. Finally, Section 5 concludes the study, discusses implications, acknowledges its limitations, and proposes directions for future research.

2. Literature review and hypotheses development

Fraud poses a significant threat to organisational sustainability by diverting critical resources, undermining efficiency, and eroding stakeholder trust (Glover & Aono, 1995). The absence of robust fraud risk assessments, coupled with the rising trend of fraud, has amplified the significance of effective fraud prevention and detection mechanisms (Halbouni et al., 2016). Fraud involves deliberate manipulation of financial statements for personal gain (Hall, 2011) and remains pervasive across industries, where ACFE (2024) categorises occupational fraud as asset misappropriation (89%), corruption (48%), and financial statement fraud (5%), with the latter causing the highest median loss of USD 766,000 per case. In an era of rising cybercrime, strengthening fraud prevention and detection mechanisms is vital to address modern fraud complexities, safeguarding the financial system (Altarraji & Mokdad, 2024; Muhammed et al., 2024).

2.1 Broad theories and models

This study adopts a multi-theoretical perspective, incorporating Agency Theory, Resource Dependence Theory, Stakeholder Theory, the Fraud Triangle, Fraud Diamond, Fraud Hexagon, the Organisational Fraud Triangle, Social Identity Theory, and Cognitive Dissonance Theory to explain the role of fraud prevention and detection tools in deterring fraud. Agency Theory suggests that conflicts of interest between principals (shareholders) and agents (managers) create incentives for opportunistic behaviour, necessitating strong monitoring in a corporate context (Jensen & Meckling, 1976). In this study, Agency Theory provides the primary

justification for the 27 traditional fraud deterrence tools, such as bank reconciliations, internal audits and corporate codes of conduct. In Sri Lankan LCs, these tools serve as vital oversight mechanisms to mitigate the agency problem by restricting the managers' ability to engage in fraudulent reporting. Complementing this, Resource Dependence Theory indicates that an organisation's adoption of specific tools is influenced by its dependency on external digital environments and financial capital (Hillman et al., 2009). This provides the basis for the 31 technological tools explored in this study. It suggests that a shift toward advanced mechanisms, including Bayesian networks, digital forensics and neural networks, is a strategic response to the complexities of the digital age and the need to secure stakeholder trust through transparent information systems. Furthermore, Stakeholder Theory expands this focus beyond shareholders to include depositors and the general public, who are significantly affected by recent Sri Lankan corporate failures (Arjoon, 2005; Freeman et al., 2004). This theory justifies the study's focus on ethical tools, such as whistleblowing policies and ethics officers, as important mechanisms to maintain multi-stakeholder integrity.

To understand how fraud is deterred, the study utilises the Fraud Triangle (Cressey, 1950) and Fraud Diamond (Wolfe & Hermanson, 2004) as frameworks to categorise the functionality of the tools examined. Specifically, traditional tools such as bank reconciliations, internal audits, and inventory observations are primarily designed to restrict the *opportunity* and *capability* dimensions by strengthening physical and procedural oversight. In contrast, technological tools, including Benford's Law, digital forensic tools and data mining, are evaluated for their ability to identify anomalies and patterns that often stem from hidden *pressure* or sophisticated *rationalisation*. These advanced tools are essential in the digital age for detecting and preventing irregularities in complex, technology-mediated transactions that traditional, routine-based oversight may overlook. Furthermore, the Fraud Hexagon (Vousinas, 2019) introduces *ego* and *collusion* as critical dimensions. This model provides the theoretical rationale for advanced technological tools, as high-level collusion often bypasses traditional routine-based controls. Advanced tools like digital forensics, neural networks and data mining are conceptually better equipped to identify the sophisticated, non-linear patterns associated with executive-level fraud. Similarly, Free (2015)'s organisational Fraud Triangle shifts the lens to *leadership*, *management control systems* and *culture*. This framework is operationalised in the study by examining how tools like codes of conduct (*culture*) and

management oversight (*leadership*) compare against technological controls. It helps justify why internal employees might favor traditional routines if the organisational culture has not yet embraced digital innovation.

Finally, Social Identity Theory and Cognitive Dissonance Theory are utilised to justify the perception gaps related to fraud risks and fraud deterrence mechanisms. Social identity theory suggests that individuals tend to interpret the usage of traditional and technological fraud deterrence mechanisms in ways that reinforce their affiliation with their professional or organisational group (Tajfel & Turner, 1979). Cognitive Dissonance Theory further explains that professionals may favour tools they are most familiar with to maintain consistency between their existing skills and their professional responsibilities (Festinger, 1957). Together, these theories explain why external auditors, who are aligned with global professional standards, and LC employees may perceive traditional and technological tools differently, given their distinct roles and daily operational responsibilities.

2.2 *Empirical evidence on the perceived level of fraud occurrence and differences in such perceptions*

Accounting scandals are on the rise globally, with developing economies being more vulnerable due to weak corporate governance and fraud prevention and detection mechanisms (Juhandi et al., 2020). Halbouni et al. (2016) emphasise that nearly half of the UAE firms have been victims of fraud, while Jayasinghe and Ajward (2019) state that overall, 76% of auditors expect fraud to increase in the Sri Lankan financial sector. Similarly, Ramesh and Vinayagathan (2024) highlight that the pervasive presence of corruption remains a systemic challenge in Sri Lanka, emphasising the crucial need for effective fraud prevention measures in emerging economies such as Sri Lanka. Tan et al. (2023) suggest that professionals' perceptions regarding governance and fraud disclosure practices significantly influence how fraud risks are interpreted and reported. Moreover, Halbouni et al. (2016) opined that there was no significant difference between financial accountants' and internal and external auditors' perceptions of their companies being fraud victims and their expectations of future fraud. Nonetheless, the dearth of studies investigating differences in perceptions among professionals regarding the level of fraud occurrence in emerging economies justifies further exploration.

From a theoretical perspective, differences in perceptions among professional groups can be explained through social psychological perspectives where the Social Identity Theory proposes that individuals tend to evaluate organisational practices in ways that reinforce their professional affiliations and group identities (Tajfel & Turner, 1979). In this context, LC employees may perceive the level of fraud occurrence differently compared to external auditors, who evaluate organisations from an independent monitoring perspective. Moreover, Cognitive Dissonance Theory advocates that individuals responsible for maintaining internal control systems may adjust their perceptions to align with their professional responsibilities and organisational roles (Festinger, 1957). Hence, differences in professional roles between listed company employees and external auditors could lead to differing perceptions of fraud, and thereby, the following hypothesis could be proposed.

H_1 : There is a significant difference in the perceived level of fraud occurrence between LC employees and external auditors.

This corresponds to the extent to which fraud prevention and detection mechanisms are utilised to deter fraud.

2.3 Empirical evidence on the perceived level of usage of traditional and technological fraud prevention and detection techniques and differences in such perceptions

Despite preventive efforts, fraud remains a persistent threat, highlighting the crucial need for comprehensive anti-fraud measures (Mangala & Kumari, 2017). ACFE (2024) emphasises that fraud was predominantly detected through whistleblowers' tips (43%), followed by internal audits (14%) and management reviews (13%). Halbouni et al. (2016) reveal that audit committees play a vital role in deterring fraud, with the internal audit function being the most influential, while external audit is also significant. Nonetheless, the rapid advancement of technology has expanded the scope of anti-fraud measures. Ali et al. (2024) propose that digital tools, including predictive analytics, real-time risk alerts, and forensic data analytics, enhance the timeliness and effectiveness of fraud detection and prevention. Othman et al. (2015) state that frequently used fraud detection and prevention tools include password and virus protection, firewalls, discovery sampling, and continuous auditing, while whistle-blowing policies, fraud hotlines, and forensic accountants are rarely used, despite their high importance.

Mahathevan (1997) opined that traditional techniques are widely accepted in deterring fraud, while Kassem and Omoteso (2024) further state that Big 4 auditors rely on traditional tools. Nevertheless, organisations should rely more on technological tools for real-time financial reporting and proactive fraud detection (Gill, 2009; Halbouni et al., 2016; Tum, 2013). Jayasinghe and Ajward (2019) reveal that integral traditional tools for fraud deterrence are internal control reviews, bank reconciliations, corporate codes of conduct, external audits, and operational audits, while password and virus protection, firewalls, and continuous auditing are integral technological controls. Analytical tools such as Benford's Law, Bayesian networks, neural networks, and data mining further strengthen proactive fraud detection and prevention (Coderre, 2006). Recent studies further emphasise the growing importance of data analytics, machine learning, and artificial intelligence in strengthening organisational fraud prevention and detection capabilities (Ngai et al., 2011; Kassem & Omoteso, 2024). Despite these advancements, many organisations in developing economies continue to rely heavily on traditional tools, often due to cost and capability constraints (Kassem & Omoteso, 2024). Though the literature emphasises the usage of both traditional and technological tools in deterring fraud and its associated costs, empirical evidence remains mixed due to differences in contexts and adoption levels of these tools.

According to Jayasinghe and Ajward (2019), perception differences exist between internal and external auditors in terms of the level of usage of certain traditional fraud prevention and detection techniques, while there are no perception differences between them in terms of software-based techniques. Omar and Bakar (2012) reveal that significant differences exist between the internal auditors' and fraud investigators' perceptions of fraud prevention mechanisms like fraud hotlines, anti-fraud policies and fraud prevention training. Othman et al. (2015), Halbouni et al. (2016), and Uecker et al. (1981) report no significant differences between internal and external auditors in their use of traditional and technological fraud prevention techniques. Thus, the literature presents mixed evidence and highlights a dearth of studies on differences in perceptions among professionals regarding the use of traditional and technological anti-fraud tools (Jayasinghe & Ajward, 2019). In this light, social psychological theories offer meaningful insights. Accordingly, Social Identity Theory suggests that professionals' strong organisational affiliation may bias their perception of their organisation's usage of fraud deterrence

techniques (Tajfel & Turner, 1979). The Cognitive Dissonance Theory (Festinger, 1957) emphasises that when individuals experience inconsistency between beliefs and responsibilities, such as being responsible for fraud deterrence while perceiving high fraud risk, they tend to adjust their perceptions to reduce discomfort. Therefore, differences in professional roles and organisational affiliations may direct listed company employees and external auditors to differently perceive the extent to which traditional and technological fraud prevention and detection techniques are utilised within listed companies. Accordingly, the following hypotheses are developed to be examined in this study.

H_2 : There is a significant difference in the perceived level of usage of traditional and technological fraud prevention and detection techniques between LC employees and external auditors.

H_{2a} : There is a significant difference in the perceived level of usage of traditional fraud prevention and detection techniques between LC employees and external auditors.

H_{2b} : There is a significant difference in the perceived level of usage of technological fraud prevention and detection techniques between LC employees and external auditors.

Overall, literature highlights a significant increase in fraud, alongside a growing reliance on both traditional and technological fraud prevention and detection techniques to address this issue. Nevertheless, empirical evidence remains contradictory regarding the use of these techniques, particularly within the emerging economy context. Moreover, there is a dearth of studies examining a wide range of traditional and technological tools for fraud deterrence or exploring differences in perceptions of fraud and the usage of fraud deterrence mechanisms among professionals. To address this empirical gap, this study investigates a wide and comprehensive suite of traditional and technological fraud prevention and detection techniques used by Sri Lankan listed companies, while also examining perceptual differences among professionals, thereby providing valuable insights into the fraud prevention and detection literature in emerging markets.

3. Research methodology

This study adopts a postpositivist research paradigm, aligned with a quantitative, deductive approach, wherein hypotheses derived from

existing theories guide the investigation, which is consistent with prior studies (Bierstaker et al., 2006; Halbouni et al., 2016; Jayasinghe & Ajward, 2019; Mangala & Kumari, 2017; N'Guilla Sow et al., 2018 and Othman et al., 2015). In collecting primary data, a survey was employed using a self-administered structured questionnaire.

3.1 Population and sample

The perceptions examined in this study were drawn from two key professional groups: top- and middle-level management employees in listed companies (LC employees), and external auditors at top and middle management levels in audit firms providing external audit services to listed companies in Sri Lanka. Listed companies were specifically targeted due to their heightened exposure to fraud and governance obligations under the Colombo Stock Exchange listing rules, which require robust fraud deterrence mechanisms in such companies (CA Sri Lanka, 2017; Halbouni et al., 2016). Increased corporate accountability has placed greater responsibility on management and auditors in combating fraud (Law, 2011; Mangala & Kumari, 2017; Uecker et al., 1981). Thus, it is evident that professionals in the top and middle management levels within organisations, as well as external auditors, are highly involved in and aware of the utilisation of fraud prevention and detection techniques, which constitutes the organisational framework for fraud deterrence. The unit of analysis, therefore, comprises LC employees and external auditors, with a sample of 127 LC employees and 102 external auditors, making a total of 229 professionals.

The inclusion of both listed company employees and external auditors is a deliberate methodological choice that allows for a comparative analysis of perceptions between two key stakeholder groups, providing insights into how insiders and outsiders perceive the use of fraud deterrence tools differently. These two groups offer unique perspectives into the fraud landscape: LC employees provide an insider perspective rooted in operational knowledge of internal controls, while external auditors provide an independent outsider lens focused on objective verification (Bierstaker et al., 2006; Othman et al., 2015). This dual-sample approach is theoretically grounded in Social Identity Theory (Tajfel & Turner, 1979), which suggests that an individual's professional identity and organisational role significantly shape their perceptions of risk and control efficacy. By comparing these groups, the study can identify critical perception gaps between those operating the systems and those auditing them. To analyse these differences, since the data is observed to be non-normal, the

study employs the Mann-Whitney U-test, a non-parametric technique specifically designed for comparing two independent groups. For such comparative analysis, the current sample size of 229 respondents (127 LC employees and 102 external auditors) is considered adequate and statistically robust. According to Siegel and Castellan (1988) and Field (2013), the Mann-Whitney U-test maintains high power and efficiency even with moderate sample sizes, and groups exceeding 100 observations are sufficient to detect significant differences without the need for massive sample sizes typically required by parametric tests. This sample size is also consistent with, or exceeds, established perception-based fraud studies (Bierstaker et al., 2006; Halbouni et al., 2016; Othman et al., 2015). Random sampling was employed to ensure representativeness across demographic characteristics, further strengthening the validity and generalisability of the comparative results (Johnson & Rudesill, 2001; Mangala & Kumari, 2017; Othman et al., 2015).

3.2 Questionnaire development

A self-administered structured questionnaire was employed in collecting data, adopted from Bierstaker et al. (2006), Halbouni et al. (2016), Law (2011), Mangala and Kumari (2017) and Othman et al. (2015), comprising three sections, where the first section gathered demographic information from both groups using multiple-choice questions. Sections two and three included five-point Likert scale questions to assess LC employees' and external auditors' perceptions of fraud and the usage of traditional and technological fraud prevention and detection mechanisms in deterring fraud. Furthermore, the occurrence of fraud was measured using a five-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree), based on statements such as "My firm has been a victim of fraud." Conversely, the usage of fraud deterrence techniques was assessed via an item-specific frequency-based scale ranging from 1 (Never) to 5 (Almost Always). This shift to a frequency-based scale for the tools section was a deliberate methodological choice to mitigate acquiescence bias by requiring respondents to report observable organisational practices rather than personal agreement (Höhne & Lenzner, 2018). Furthermore, the employment of positively phrased statements in the questionnaire design is a standard and validated practice in established fraud perception research (Bierstaker et al., 2006; Halbouni et al., 2016; Jayasinghe & Ajward, 2019; Othman et al., 2015). The questionnaire, developed based on an extensive literature survey, was validated through expert reviews and a pilot

survey to ensure face validity and clarity, and the final version was distributed electronically.

3.3 Data analysis strategies

The collected data were cleaned and screened for missing values, errors, and outliers. Descriptive statistics, the one-sample Wilcoxon signed rank test, mean ranking and Mann-Whitney U test were applied to assess perceptions of fraud occurrence and the usage of traditional and technological fraud prevention and detection techniques, as well as differences in such perceptions between LC employees and external auditors. Thus, this methodology ensures the collection of reliable, valid, and representative data while addressing the key research objectives.

4. Empirical results and discussion

4.1 Demographic profile of the respondents

As per the overview of respondents' demographic characteristics presented in Table 1, out of 229 respondents, 127 are LC employees (55.5%) while 102 are external auditors (44.5%). Males dominated both groups (approximately 70%). The age distribution shows that most of the LC employees are aged 30-49 years (78%), with no employees aged 70 years or above, while most external auditors are younger, aged between 20-39 years (69.6%). With respect to academic qualifications, most of the LC employees hold postgraduate qualifications: MBA, MSc, or MPhil (58.3%), while external auditors are mainly bachelor's degree holders (52.9%). Nearly all respondents are professionally qualified: LC employees 96.9%, external auditors 99%. In terms of roles, LC employees mainly serve as finance managers (28.3%), while the remainder hold various managerial and executive positions, including internal audit managers, general managers, and CFOs, whereas most of the external auditors are audit managers (29.4%) and partners (28.4%). A substantial portion of LC employees are experienced professionals with over 15 years of work experience (50.4%), while the majority of the external auditors possess 2-5 years of work experience (30.4%). Among LC employees, 76.4% work in companies with over 300 employees, whereas 68.6% of external auditors are affiliated with Big 4 audit firms. Moreover, 51.2% of LC employees are part of the top management level, with 48.8% representing the middle management level. Based on the area of company's operations, 76.4% of the LC employees are from LCs that operate as local companies. Given the sample's heterogeneity and

diverse representation of the respective population, it ensures that the findings are unbiased and reliable.

Table 1: Demographic Profile of the Respondents

Variable	Categories	LC employees		External auditors	
		N	%	N	%
Role	LC employees / External auditors of LCs	127	55.5	102	44.5
Gender	Male	89	70.1	74	72.5
	Female	38	29.9	28	27.5
	Total	127	100	102	100
Age	20-29 Years	13	10.2	40	39.2
	30-39 Years	50	39.4	31	30.4
	40-49 Years	49	38.6	14	13.7
	50-59 Years	10	7.9	7	6.9
	60-69 Years	5	3.9	7	6.9
	70 Years & above	-	-	3	2.9
	Total	127	100	102	100
Highest Academic Qualification	G.C.E. O/L	-	-	1	1
	G.C.E. A/L	6	4.7	15	14.7
	Certificate Level	-	-	1	1
	Diploma Level	4	3.1	-	-
	Bachelor's Degree	38	29.9	54	52.9
	Postgraduate Diploma	5	3.9	2	2
	MBA/ MSc/ MPhil	74	58.3	27	26.5
	Doctor of Philosophy	-	-	2	2
	Total	127	100	102	100
Professional Qualifications	Professionally Qualified	123	96.9	101	99
	Not Professionally Qualified	4	3.1	1	1
	Total	127	100	102	100
Current Position	CEO	3	2.4		
	COO	3	2.4		
	CFO	13	10.2		
	CRO (Chief Risk Officer)	4	3.1		
	CLO (Chief Legal Officer)	5	3.9		
	CIA (Chief Internal Auditor)	8	6.3		
	General Manager	15	11.8		
	Finance Director	5	3.9		
	Financial Controller	9	7.1		
	Senior Internal Audit Manager	7	5.5		
	Finance Manager	36	28.3		
	Internal Audit Manager	16	12.6		

Variable	Categories	LC employees		External auditors	
		N	%	N	%
	Assistant Internal Audit Manager	3	2.4		
	Total	127	100		
	Partner			29	28.4
	Director			8	7.8
	Senior Audit Manager			15	14.7
	Audit Manager			30	29.4
	Assistant Audit Manager			20	19.6
	Total			102	100
Work Experience	Less than 2 Years	4	3.1	10	9.8
	2-5 Years	10	7.9	31	30.4
	6-10 Years	26	20.5	22	21.6
	11-15 Years	23	18.1	13	12.7
	More than 15 Years	64	50.4	26	25.5
	Total	127	100	102	100
Company Size	Less than 50 Employees	4	3.1		
	50 - 300 Employees	26	20.5		
	More than 300 Employees	97	76.4		
	Total	127	100		
Size of the Audit Firm	Big 4 Audit Firm	70	68.6		
	Non-Big 4 Audit Firm	32	31.4		
	Total	102	100		
Management Level	Top-Level Management	65	51.2		
	Middle-Level Management	62	48.8		
	Total	127	100		
Area of Company's Operations	Local Company	97	76.4		
	International Company	25	19.7		
	Regional Company	5	3.9		
	Total	127	100		

Source(s): Author constructed

4.2 *Perceptions of the existence of fraud in LCs and differences in such perceptions*

The descriptive statistics and one-sample Wilcoxon signed rank test results related to the perceived level of fraud occurrence in LCs are depicted in Table 2.

Table 2: Descriptive Statistics & One-Sample Wilcoxon Signed Rank Test - Perceptions of Fraud in LCs

Role	N	Mean	Median	SD	z-value	p-value ^a
LC Employees	127	3.52	4.00	1.227	4.462	0.000**
External Auditors of LCs	102	3.67	4.00	1.047	5.567	0.000**

Source(s): Author constructed

Note(s): ** $p < 0.01$

^a Based on the one-sample Wilcoxon signed rank test performed, the significance of the difference between the test value of 3 and the median values are indicated, where ** $p < 0.01$.

Both the LC employees ($Mean=3.52$, $Median=4$, $p < 0.01$) and external auditors ($Mean=3.67$, $Median=4$, $p < 0.01$) significantly perceive that fraud exists within LCs with a median rating of 4 which is above the midpoint, i.e., 3 on the five-point Likert scale. This indicates strong agreement across both LC employees and external auditors that fraud exists in LCs. The results are consistent with those of previous studies by Halbouni et al. (2016) for the UAE and Bierstaker et al. (2006) for the USA, which revealed widespread fraud in corporate entities and anticipated an increase in future fraud occurrences. Similarly, Jayasinghe and Ajward (2019) highlight that fraud does exist in Sri Lankan banking and finance institutions, while Birol (2019), Othman et al. (2015) and Rostami and Rezaei (2021) indicate fraud as a serious global problem. Further, Rathnasiri and Bandara (2017) highlight an increasing trend of financial crimes in Sri Lanka in recent years, reinforcing the study's findings.

In testing the first research hypothesis (H_1) of the study: "there is a significant difference in the perceived level of fraud occurrence between LC employees and external auditors", the Mann-Whitney U test is conducted, and the results are presented in Table 3.

Table 3: Mann-Whitney U test: Perceptions of Fraud in LCs

Existence of fraud in LCs	N	Mean Rank	z-value	p-value
LC employees	127	112.50	-0.659	0.510
External auditors of LCs	102	118.12		

Source(s): Author constructed

Note(s): ** $p < 0.01$

The results indicate no statistically significant difference between LC employees' and external auditors' perceptions of fraud occurrence in LCs ($p > 0.05$). Thus, the first research hypothesis (H_1),

which proposed a significant difference between LC employees' and external auditors' perceptions of fraud occurrence in LCs, is not supported and implies that both professionals similarly perceive that fraud exists in LCs, exhibiting a shared awareness of corporate vulnerabilities. This finding is consistent with Halbouni et al. (2016), who opined that there are no significant perceptual differences among financial accountants, internal and external auditors regarding the existence of fraud in UAE. From Stakeholder Theory perspective, this alignment in perceptions suggests that, despite their differing organisational roles, both groups demonstrate a shared awareness of fraud-related risks. Such alignment is essential for strengthening organisational accountability, particularly in emerging market contexts where regulatory enforcement and monitoring mechanisms may be less effective (World Bank, 2024; Freeman et al., 2021).

4.3 *Perceptions of the usage of traditional and technological fraud prevention and detection tools in LCs and differences in such perceptions*

Accordingly, as per the results in Table 4, LC employees perceive that traditional fraud prevention and detection tools (*TradTools*) are being utilised in LCs to deter fraud, with a median of 4.07, which is above the midpoint of 3 on the five-point Likert scale ($Mean=4.10$, $p<0.01$). Based on the mean ranking, the most widely used traditional tools, as perceived by LC employees, are bank reconciliations, account reconciliations, cash reviews, inventory observations, and internal audits, all with mean values above 4.4 and median values of 5. The least utilised *TradTools* are dedicated fraud departments, organisational use of forensic accountants, investigative media, employee counselling programmes and whistleblowing policies. Nevertheless, the existence of a dedicated fraud department is not statistically significant ($p>0.05$), with a median value of 3, being the least utilised traditional tool. Therefore, it is evident that LC employees generally agree that all 26 traditional tools presented in Table 4 are utilised in LCs for fraud prevention and detection, while they are neutral regarding the usage of dedicated fraud departments as a traditional fraud control measure.

As shown in Table 4, external auditors moderately agree on the use of traditional tools in LCs in deterring fraud, with a median of 3.76, which is significantly different from the midpoint of 3 ($Mean=3.67$, $p<0.01$). Thus, it indicates that both the LC employees and external auditors perceive that traditional tools are utilised in LCs in preventing and detecting fraud. Meanwhile, external

auditors ranked bank reconciliations, internal audits, external audits, inventory observations and account reconciliations as most widely utilised traditional tools, with mean values of 4 or above and median values of 4. Overall, both LC employees and external auditors rank the same *TradTools*: bank reconciliations, internal audit, inventory observations, and account reconciliations as highly utilised in LCs, with slight differences in ranking, except for external audit, which is ranked differently by both groups. Furthermore, when considering the least utilised *TradTools*, external auditors also ranked the same set of tools: dedicated fraud departments, organisational use of forensic accountants, investigative media, employee counselling programmes and whistleblowing policies as least utilised, although their rankings are slightly different, confirming a consistent pattern across the perspectives of both groups. Additionally, as perceived by external auditors, the organisational use of forensic accountants, dedicated fraud departments and investigative media is not statistically significant ($p>0.05$), being the least utilised traditional tools.

Table 4: LC Employees' and External Auditors' Perceptions of Traditional Fraud Prevention and Detection Tools

Traditional fraud prevention and detection tools (<i>TradTools</i>)	LC employees				External auditors			
	Mean	Median	<i>p</i> -value ^a	Rank	Mean	Median	<i>p</i> -value ^a	Rank
Bank reconciliations	4.61	5.00	0.000**	1	4.24	4.00	0.000**	1
Account reconciliation	4.52	5.00	0.000**	2	3.99	4.00	0.000**	5
Cash reviews	4.51	5.00	0.000**	3	3.97	4.00	0.000**	6
Inventory observations	4.43	5.00	0.000**	4	4.03	4.00	0.000**	4
Internal audit	4.36	5.00	0.000**	5	4.13	4.00	0.000**	2
Management review	4.26	4.00	0.000**	6	3.81	4.00	0.000**	7
Document examination	4.23	4.00	0.000**	7	3.71	4.00	0.000**	13
Sound internal control systems/ Internal control review and improvement	4.23	4.00	0.000**	7	3.8	4.00	0.000**	8
Surveillance equipment	4.22	4.00	0.000**	9	3.59	4.00	0.000**	16
Surprise audits	4.21	4.00	0.000**	10	3.49	4.00	0.000**	18
Risk management process	4.17	4.00	0.000**	11	3.76	4.00	0.000**	11
Reference checks on employees	4.05	4.00	0.000**	12	3.7	4.00	0.000**	14

Traditional fraud prevention and detection tools (TradTools)	LC employees				External auditors			
	Mean	Median	p-value ^a	Rank	Mean	Median	p-value ^a	Rank
Exception reporting/ Suspicious transaction reporting	4.04	4.00	0.000**	13	3.48	4.00	0.000**	20
Corporate code of conduct (Ethics policy)	4.02	4.00	0.000**	14	3.72	4.00	0.000**	12
Employment contracts	4.02	4.00	0.000**	14	3.77	4.00	0.000**	10
Increased role of the audit committee	4.02	4.00	0.000**	14	3.78	4.00	0.000**	9
Corporate security	3.98	4.00	0.000**	17	3.62	4.00	0.000**	15
External audit	3.97	4.00	0.000**	18	4.13	4.00	0.000**	2
Sound ethical culture/ Ethics officer	3.88	4.00	0.000**	19	3.53	4.00	0.000**	17
Anti-fraud policy/ A strategy to combat fraud	3.87	4.00	0.000**	20	3.32	3.00	0.003**	21
Change of personnel/ duties	3.76	4.00	0.000**	21	3.49	3.00	0.000**	18
Fraud prevention and detection training	3.72	4.00	0.000**	22	3.28	3.00	0.008**	22
Whistleblowing policy (anonymous letters)	3.57	4.00	0.000**	23	3.27	3.00	0.003**	23
Employee counselling programs	3.53	4.00	0.000**	24	3.27	3.00	0.014**	23
Investigative media	3.52	4.00	0.000**	25	3.14	3.00	0.278	25
Organizational use of forensic accountants	3.47	4.00	0.001**	26	3.03	3.00	0.724	27
Dedicated fraud department, function, or team	3.24	3.00	0.108	27	3.1	3.00	0.449	26
Overall average: Traditional fraud prevention and detection tools (TradTools)	4.0983	4.0741	0.000**		3.6714	3.7593	0.000**	

Source(s): Author constructed

Note(s): ** $p < 0.01$

aBased on the one-sample Wilcoxon signed rank test performed, the significance of the difference between the test value of 3 and the median values are indicated, where ** $p < 0.01$.

These findings align with those of Halbouni et al. (2016) and McKee (2006), who indicate that financial accountants and internal and external auditors hold positive perceptions of the roles played by

both traditional and technological tools in preventing and detecting fraud. Mahathevan (1997) posits that traditional techniques are widely acceptable and employed in organisations in deterring fraud. Moreover, this study's findings align with ACFE (2018), Bierstaker et al. (2006), Jayasinghe and Ajward (2019), Mangala and Kumari (2017), Othman et al. (2015), Peiris and Aruppala (2021), and Rahman and Anwar (2014), who reveal that internal audits, audit committees, external audits, bank reconciliations, cash verifications, and inventory observations remain dominant fraud prevention and detection tools in corporations. Conversely, despite the high importance, the limited use of forensic accountants, fraud hotlines, employee counselling programmes, and whistle-blowing policies is in line with Othman et al.'s (2015) argument that lack of specialised expertise and inadequate whistleblower protection hinder broader adoption of such tools. Further, Rustiarini and Sunarsih (2017) argue that in other Asian societies, individual whistleblowing intentions are heavily influenced by perceived social pressure and the level of formal organisational support. Hence, the high utilisation of traditional tools, including bank reconciliations and internal audits, suggests that Sri Lankan LCs have management control systems that are deeply rooted in conventional oversight. Nevertheless, the significantly lower utilisation of ethical tools like whistleblowing policies and dedicated fraud departments indicates a potential weakness in the organisational *culture* dimension of Free's (2015) organisational Fraud Triangle model. This reflects a Resource Dependence constraint where firms prioritise low-cost manual oversight over high-investment cultural frameworks (Indrayani et al., 2025). This imbalance suggests that while LCs are technically monitoring transactions, they may not be adequately addressing the *cultural* and *leadership* failures that allow fraud to thrive.

Table 5 presents perceptions of the usage of technological fraud prevention and detection tools (*TechTools*) in deterring fraud in LCs. LC employees moderately agree that technological tools are utilised in LCs, with a median of 3.58, which is statistically significantly different from the midpoint of 3 on the five-point Likert scale ($Mean=3.67, p<0.01$). The most widely used *TechTools*, as perceived by LC employees, are firewalls, password protection, virus protection, filtering software and continuous auditing, with mean values of above 4 and median values of 5. On the other hand, Bayesian network, Benford's Law, regression analyses, digital forensic tools, correlation analyses and neural networks are the least utilised technological tools with comparatively lower mean values among all

thirty-one technological fraud prevention and detection techniques. Further, discovery sampling, statistical software for fraud detection, artificial intelligence, fraud detection software, decision trees, and discriminant analysis are not significant ($p>0.05$).

External auditors' perceptions indicate a more positive inclination regarding the utilisation of technological tools in LCs, rather than being strictly neutral, with a median of 3.3, which is statistically significantly different from the midpoint of 3 ($Mean=3.44$, $p<0.01$). Thus, it is evident that both LC employees and external auditors perceive that technological tools are utilised in LCs to prevent and detect fraud. Moreover, reflecting similar trends, external auditors also perceive the same set of technological tools as highly utilised, although the rankings are slightly different: password protection, firewalls, virus protection, continuous auditing and filtering software. On the other hand, both groups similarly rank the least utilised TechTools in LCs: Bayesian network, Benford's Law, regression analyses, correlation analyses, neural networks and digital forensic tools, with minor differences in ranking. Thus, it is evident that both LC employees and external auditors rely on basic technological tools rather than advanced analytical tools, indicating relatively limited technological sophistication among Sri Lankan LCs in fraud deterrence. The limited adoption of advanced technological tools can be explained through the Resource Dependence Theory (Hillman et al., 2009). Organisations in emerging economies like Sri Lanka are often dependent on external providers for advanced technological infrastructure and specialised skills like digital expertise and forensic software that are necessary to transition from basic password protection to proactive, AI-driven deterrence. Furthermore, from a Fraud Hexagon perspective, the absence of these advanced tools represents a significant opportunity gap; while traditional tools may detect simple theft, they are ill-equipped to detect complex *collusion* and *ego*-driven fraud that advanced analytics are designed to uncover (Vousinas, 2019). Coderre (2006) argues that advanced analytical techniques are vital in detecting fraud in organisations. Nevertheless, as perceived by external auditors, several technological tools are not statistically significant ($p>0.05$), indicating limited or inconsistent usage across LCs.

These findings align with Bierstaker et al. (2006), Halbouni et al. (2016) and Zhou and Kapoor (2011), who emphasise that tools and techniques that embed information technology are effective in combating fraud in organisations. Prior studies further indicate that firewalls, virus protection, password protection, filtering software and

continuous auditing are the most common technological techniques employed by firms, while Bayesian networks, Benford's Law, neural networks, and discovery sampling are the least utilised (Halbouni et al., 2016; Jayasinghe & Ajward, 2019; Othman et al., 2015; Peiris & Aruppala, 2021). Nevertheless, these results contradict with Phua et al. (2010), who argue that logistic models, neural networks, Bayesian networks, and decision trees are the most utilised technological fraud controls. Bierstaker et al. (2006) emphasise that continuous auditing is a less often utilised technological technique, while Jayasinghe and Ajward (2019) highlight discovery sampling as a frequently used tool in the public sector. In addition, Zhou and Kapoor (2011) suggest that regression analyses, decision trees, neural networks, and Bayesian networks are widely used *TechTools*, whereas the present findings indicate that such techniques are rarely applied in the Sri Lankan context. Thus, prior studies reveal divergent perspectives on the most and least utilised traditional and technological fraud prevention and detection techniques, leading to mixed empirical evidence.

Table 5: LC Employees' and External Auditors' Perceptions of Technological Fraud Prevention and Detection Tools

Technological fraud prevention and detection tools (<i>TechTools</i>)	LC employees				External auditors			
	Mean	Median	<i>p</i> -value ^a	Rank	Mean	Median	<i>p</i> -value ^a	Rank
Firewalls	4.55	5.00	0.000**	1	4.13	4.00	0.000**	2
Password protection	4.53	5.00	0.000**	2	4.17	4.00	0.000**	1
Virus protection	4.47	5.00	0.000**	3	4.09	4.00	0.000**	3
Filtering software	4.4	5.00	0.000**	4	3.83	4.00	0.000**	5
Continuous auditing	4.24	5.00	0.000**	5	3.85	4.00	0.000**	4
System analysis/audit	4.18	4.00	0.000**	6	3.69	4.00	0.000**	8
IT-related internal controls	4.15	4.00	0.000**	7	3.74	4.00	0.000**	6
Ratio analysis/ Financial ratios analysis software	4.12	4.00	0.000**	8	3.72	4.00	0.000**	7
Microsoft Excel functionalities in fraud prevention and detection	3.76	4.00	0.000**	9	3.66	4.00	0.000**	9
Random sampling	3.71	4.00	0.000**	10	3.53	4.00	0.000**	11
Data encryption	3.69	4.00	0.000**	11	3.62	4.00	0.000**	10
Data mining	3.55	4.00	0.000**	12	3.23	3.00	0.028**	17
Surveillance of electronic correspondence	3.51	4.00	0.000**	13	3.26	3.00	0.015**	16
Whistleblowing hotline (anonymous calls/emails)	3.47	3.50	0.000**	14	3.23	3.00	0.033**	17

	LC employees				External auditors			
Technological fraud prevention and detection tools (<i>TechTools</i>)	Mean	Median	<i>p</i> -value ^a	Rank	Mean	Median	<i>p</i> -value ^a	Rank
Data visualisation (Microsoft Power BI, Tableau, Spotfire)	3.47	4.00	0.000**	14	3.37	3.00	0.003**	13
Pivot table analysis	3.45	4.00	0.001**	16	3.39	3.00	0.001**	12
Gap analysis	3.45	4.00	0.001**	16	3.27	3.00	0.019**	15
Duplicate testing	3.32	3.00	0.028**	18	3.35	3.00	0.003**	14
Intrusion detection and prevention system	3.31	3.00	0.028**	19	3.19	3.00	0.095	19
Discovery sampling	3.29	3.00	0.06	20	3.19	3.00	0.07	19
Statistical software that can be used to detect fraud (R Programming, Python, SAS, QlikView, SAP, SAI Global, Oracle)	3.1	3.00	0.459	21	3.07	3.00	0.569	22
Artificial intelligence	3.05	3.00	0.762	22	3.02	3.00	0.868	23
Fraud detection software: IDEA, ACL	3.01	3.00	0.97	23	3.15	3.00	0.179	21
Decision trees	2.82	3.00	0.118	24	2.96	3.00	0.81	24
Discriminant analysis	2.77	3.00	0.074	25	2.96	3.00	0.723	24
Neural networks	2.71	3.00	0.039**	26	2.92	3.00	0.498	27
Correlation analysis	2.68	3.00	0.01**	27	2.88	3.00	0.44	28
Digital forensic tools: Forensic Toolkit (FTK), EnCase, Computer Online Forensic Evidence Extractor (COFEE), Bulk_Extractor, WindowsSCOPE	2.64	3.00	0.009**	28	2.94	3.00	0.684	26
Regression analysis	2.5	3.00	0.000**	29	2.82	3.00	0.157	29
Benford's Law	2.41	2.00	0.000**	30	2.78	3.00	0.113	30
Bayesian network	2.39	2.00	0.000**	31	2.76	3.00	0.049**	31
Overall average: Technological fraud prevention and detection tools (<i>TechTools</i>)	3.6728	3.5806	0.000**		3.4418	3.2903	0.000**	

Source(s): Author constructed

Note(s): ***p*<0.01

aBased on the one-sample Wilcoxon signed rank test performed, the significance of the difference between the test value of 3 and the median values are indicated, where ***p*<0.01.

In addition, according to the results presented in Tables 4 and 5, it is evident that both LC employees and external auditors exhibit a relatively stronger reliance on traditional tools than on technological tools in deterring fraud in LCs. This finding is consistent with prior studies conducted in emerging economies, which report that organisations often rely on established internal control mechanisms such as internal audits, bank reconciliations, and management reviews due to cost considerations and limited technological expertise (Bierstaker et al., 2006; Halbouni et al., 2016). The continued reliance on traditional mechanisms may also reflect regulatory requirements and the familiarity of listed companies with conventional audit practices (Kassem & Higson, 2012; Othman et al., 2015). Nonetheless, the relatively limited adoption of advanced analytical tools suggests that listed companies may not yet fully leverage emerging technologies capable of enhancing proactive fraud prevention and detection (Ngai et al., 2011; Kassem & Omoteso, 2024). This continued dominance of traditional tools further indicates that the organisational *culture* and *management control systems* in Sri Lankan LCs are still rooted in conventional oversight (Free, 2015), potentially creating vulnerabilities to complex fraud risks arising from *ego* and *collusion* highlighted in the fraud hexagon, which traditional tools are less likely to detect. Moreover, the predominant usage of traditional tools suggests that Sri Lankan LCs focus heavily on restricting the *opportunity* element of the Fraud Diamond. Nevertheless, these manual interventions are often insufficient to counter the *capability* (Wolfe & Hermanson, 2004) of modern fraudsters. In the digital age, *capability* is no longer just about organisational position, but rather about technological expertise. Therefore, the moderate usage of technological tools identified in this study indicates a potential vulnerability: while firms are restricting traditional *opportunities*, they remain exposed to individuals with digital *capabilities* who can bypass traditional controls.

Based on the perspectives of LC employees, among the top twenty fraud control tools employed in LCs (not tabulated), 60% are traditional tools, and 40% are technological tools. Conversely, according to external auditors, 65% are traditional tools, and 35% are technological tools (not tabulated). Thus, according to both LC employees and external auditors, within the top twenty tools, traditional tools exhibit a higher representation than technological tools, reaffirming that LCs mostly use traditional tools compared to technological tools. This finding can also be construed through fraud theory frameworks, including the Fraud Triangle and Fraud Hexagon, which suggest that monitoring and control mechanisms

play a crucial role in reducing *opportunities* for fraudulent behaviour (Cressey, 1950; Vousinas, 2019). Moreover, the high reliance on traditional fraud prevention and detection techniques indicates that organisations prioritise established fraud deterrence mechanisms in managing fraud risks, despite the growing complexity of fraud in digital environments. This highlights the importance of integrating advanced technological tools. However, this reliance may be attributed to constraints such as limited financial resources and expertise, which hinder the adoption of such technologies (Bierstaker et al., 2006). Accordingly, this reflects a transitional stage in Sri Lankan corporate fraud management, where traditional tools remain dominant, while technological adoption continues to evolve. This confirms the argument of Mahathevan (1997) that traditional techniques are widely acceptable and utilised in organisations, while it contradicts with Halbouni et al. (2016) and Malaescu and Sutton (2015), who argue that the usage of technological tools is slightly higher than that of traditional tools in deterring fraud. Thus, the moderate utilisation of technological tools may increase organisations' propensity to become victims of future crimes (Halbouni et al., 2016). Therefore, professionals should be encouraged to rely more on technological tools than traditional tools to deter fraud on a real-time basis (Halbouni et al., 2016).

Table 6: Perceptions of the Level of Usage of Overall Traditional and Technological Tools

Usage of traditional/ technological fraud prevention and detection techniques in LCs	z-value	p-value	Respondent category	Mean rank
Usage of overall traditional fraud prevention and detection techniques between LC employees and external auditors	-4.300	0.000**	LC employees	131.87
			External auditors	94
Usage of overall technological fraud prevention and detection techniques between LC employees and external auditors	-1.622	0.105		

Source(s): Author constructed

Note(s): ** $p < 0.01$

To examine the second hypothesis (H_2) of the study: “there is a significant difference in the perceived level of usage of traditional and technological fraud prevention and detection techniques between LC employees and external auditors”, the study employed

the Mann-Whitney U test as presented in Table 6. The results reveal a statistically significant difference between LC employees' and external auditors' perceived usage of overall traditional tools in LCs ($p < 0.01$). LC employees' perceptions of the usage of *TradTools* in LCs are statistically significantly higher than (Mean Rank=131.87) the external auditors (Mean Rank=94). Thus, the first sub-hypothesis: H_{2a} of the second research hypothesis (H_2), which examines the differences between LC employees' and external auditors' perceptions of the level of usage of traditional tools in LCs, is supported. This finding aligns with Jayasinghe and Ajward (2019), who opined that perception differences do exist between professionals in terms of the usage of certain traditional tools, yet contrast with Halbouni et al. (2016), Othman et al. (2015) and Uecker et al. (1981), who found no significant differences. The significant perception difference between these two professional groups, related to the use of traditional tools can be interpreted using Social Identity and Cognitive Dissonance theories. Social Identity Theory proposes that LC employees, identifying closely with their organisation, are more likely to perceive higher usage of traditional techniques to reinforce a sense of effectiveness and competence in deterring fraud in LCs (Tajfel & Turner, 1979). In contrast, external auditors, functioning as outsiders, are more likely to maintain professional scepticism and evaluate the same tools more critically (Kassem & Omoteso, 2024; Mandal & Amilan, 2025). Cognitive Dissonance Theory suggests that LC employees who perceive the existence of fraud in LCs may exhibit a motivated bias in reporting higher usage of traditional tools, as a way to reduce the psychological tension between their role in fraud deterrence and the acknowledged risk of fraud within their organisations (Festinger, 1957). These theoretical insights offer a deeper behavioural understanding of the observed perception differences related to traditional tools usage. Nevertheless, when examining individual traditional tools (not tabulated), external audits, dedicated fraud departments and employee counselling programmes show no statistically significant difference between the perceptions of LC employees and external auditors ($p > 0.05$), while all other individual traditional tools show a statistically significant difference between their perceptions ($p < 0.05$). These findings contradict with the findings of Jayasinghe and Ajward (2019), who argue that significant differences exist between the perceptions of professionals related to the use of *TradTools* like employee counselling programmes and external audits. Conversely, perceptions of the usage of overall technological tools do not differ

significantly between LC employees and external auditors ($p>0.05$). Thus, the second sub-hypothesis, H_{2b} , that examines whether there is a significant difference in the perceived level of use of technological tools between LC employees and external auditors, is not supported. This confirms that both groups similarly perceive technological tools, due to their standardised and automated nature. Nevertheless, several individual TechTools (not tabulated), such as system audits, financial ratios analysis software, IT-related internal controls, data mining, virus protection, password protection, firewalls, filtering software, continuous auditing, Bayesian network and Benford's Law demonstrate statistically significant perception differences ($p<0.05$) while others do not. These results align with Halbouni et al. (2016), Jayasinghe and Ajward (2019), Othman et al. (2015) and Uecker et al. (1981), who highlight no significant differences between professionals in terms of technological tools usage, though it contradicts with Arens et al. (2012), who argue that internal auditors should depend more on technological tools than external auditors. Conversely, the absence of a perceptual difference in the use of technological tools suggests that automated systems may offer a more objective and standardised basis for fraud prevention and detection, thereby reducing the influence of psychological biases typically associated with traditional tools (Mandal & Amilan, 2025). Thus, it is clear that there is mixed evidence on perception differences between professionals regarding the usage of traditional and technological fraud deterrence tools, and there is a dearth of research in this area (Jayasinghe & Ajward, 2019).

4.4 *Summary of Empirical Findings*

Table 7 provides a consolidated overview of the study's findings, linking the research dimensions to their statistical outcomes and hypothesis results. This summary facilitates a clearer assessment of professionals' perceptions of fraud prevalence and the usage of traditional and technological tools in deterring fraud in listed companies. As shown in Table 7, there is a clear consensus on the high prevalence of fraud within LCs. Moreover, both LC employees and external auditors perceive greater reliance on traditional fraud deterrence tools compared to technological tools. Within the technological tools, usage is heavily skewed toward basic tools such as firewalls and password protection rather than advanced analytical tools such as digital forensics or neural networks. This pattern of adoption suggests that, while LCs are proactive in traditional defense, a significant technological gap persists in the adoption of more sophisticated digital fraud prevention and detection techniques.

Table 7: Summary of Key Findings

Research Dimension	Key Finding	Statistical Evidence	Hypothesis Result
Perception of Fraud Existence	Both groups perceive fraud prevalence to be high	LC Employees: <i>Mean</i> =3.52, <i>Median</i> =4, <i>p</i> =0.000** External Auditors: <i>Mean</i> =3.67, <i>Median</i> =4, <i>p</i> =0.000**	
Perceptual Gap regarding the existence of fraud	No significant difference in perceptions of fraud existence	<i>z</i> =-0.659, <i>p</i> =0.510	<i>H</i> ₁ : Not Supported
Traditional Tool Usage	LC Employees: High level of usage External Auditors: Moderate level of usage	<i>Mean</i> =4.10, <i>Median</i> =4.07, <i>p</i> =0.000** <i>Mean</i> =3.67, <i>Median</i> =3.76, <i>p</i> =0.000**	
Technological Tool Usage	LC Employees: Moderate level of usage External Auditors: Moderate level of usage	<i>Mean</i> =3.67, <i>Median</i> =3.58, <i>p</i> =0.000** <i>Mean</i> =3.44, <i>Median</i> =3.3, <i>p</i> =0.000**	
Perceptual Gap: <i>TradTools</i>	LC Employees perceive significantly higher usage of <i>TradTools</i> than external auditors	<i>z</i> =-4.300, <i>p</i> =0.000**	<i>H</i> _{2a} : Supported
Perceptual Gap: <i>TechTools</i>	No significant difference in how both perceive <i>TechTool</i> usage	<i>z</i> =-1.622, <i>p</i> =0.105	<i>H</i> _{2b} : Not Supported

Source(s): Author constructed

Note(s): ***p*<0.01

^a Based on the one-sample Wilcoxon signed rank test performed, the significance of the difference between the test value of 3 and the median values are indicated, where ***p*<0.01.

5. Conclusion

Fraud remains a persistent challenge globally, yet its manifestations differ significantly across institutional contexts. In developed economies, fraud deterrence is often supported by mature regulatory frameworks and advanced technological integration; conversely, in emerging economies such as Sri Lanka, the incidence and impact of fraud are exacerbated by weak regulatory enforcement and limitations in monitoring and oversight mechanisms (KPMG, 2023; World Bank, 2024). Thus, this study assessed the perceived level of fraud occurrence and the usage of traditional and technological fraud

prevention and detection techniques, along with the differences in such perceptions between LC employees and external auditors. By doing so, the study bridges a critical gap in the literature regarding the usage of a wide and comprehensive suite of traditional and technological fraud deterrence tools in a digital age within an emerging-market context. The findings confirm that both LC employees and external auditors perceive that fraud exists in LCs, with no statistically significant difference in their perceptions. From the perspective of Stakeholder Theory, this perceptual convergence is noteworthy; it suggests that despite their different organisational roles, there is an alignment in risk awareness, which is essential for organisational accountability and the protection of broader stakeholder interests (Freeman et al., 2021; Parmar et al., 2010). Furthermore, this validates the monitoring mechanisms justified by Agency Theory, as both groups recognise the pervasive nature of opportunistic behavior in the absence of stringent controls. Regarding fraud deterrence tools, the study reveals a predominant reliance on traditional tools, such as bank reconciliations, internal audits, and inventory observations. This aligns with the findings of Mangala and Kumari (2017) regarding the cost-efficiency of internal audits. From a theoretical perspective, the heavy reliance on traditional tools addresses the *opportunity* and *capability* dimensions of the Fraud Triangle and Fraud Diamond models (Cressey, 1950; Wolfe & Hermanson, 2004). Nevertheless, the lower utilisation of traditional tools such as whistleblowing policies and fraud departments, likely due to organisational capacity constraints (Othman et al., 2015), suggests a deficit in the ethical *culture* and *management control systems* as highlighted in Free's (2015) Organisational Fraud Triangle. Technological tools were perceived as only moderately employed, with a preference for basic tools: password protection and firewalls, over advanced analytics: Benford's Law, digital forensic tools and neural networks. This reflects the Resource Dependence Theory and findings by ACFE (2022) and KPMG (2019), suggesting that organisations in emerging markets remain constrained by a lack of specialised technological capital and the absence of coercive regulatory mandates to adopt advanced forensic tools (ACFE, 2024; Indrayani et al., 2025). This creates a technological lag where firms rely on traditional tools to combat emerging, complex frauds as identified in the Fraud Hexagon, which are driven by *collusion* and *ego*. Finally, the significant difference in perceived use of traditional tools between LC employees and external auditors can be explained through Social Identity Theory (Tajfel & Turner, 1979), which

suggests that employees' proximity to internal processes may induce overconfidence bias (Berthet, 2022), leading them to overestimate the effectiveness of existing controls in order to protect their professional self-concept, whereas external auditors maintain the professional skepticism necessary for objective verification. Conversely, the absence of a perception gap in technological tools indicates that standardised, automated systems provide more objective indicators for identifying potential frauds (Zhou & Kapoor, 2011). As noted by Mandal and Amilan (2025), while external auditors maintain professional skepticism, the transparent nature of technological controls reduces the psychological bias inherent in human-led traditional controls, leading to a convergence of perceptions.

This study's contribution spans multiple dimensions. Theoretically, the research provides an integrative evaluation of how fraud deterrence mechanisms align with the complex fraud landscape of emerging economies. By applying the Fraud Hexagon framework, the study illustrates a notable gap between theory and practice: while the framework highlights sophisticated behavioural elements such as *collusion* and *ego* as primary risks in modern corporate environments, the results show that deterrence remains heavily anchored in traditional mechanisms. This suggests that current deterrence strategies are potentially ill-equipped to address the specific drivers of fraud emphasised in contemporary theories. Further, the study contributes to Social Identity Theory by empirically validating how professional roles create distinct perceptual apertures. The significant perception gap identified between LC employees and external auditors regarding traditional tools suggests that organisational proximity can influence how these controls are applied and interpreted: a concept that enriches the literature on how professional roles influence the perception of fraud controls in organisations. In terms of methodological contributions, this study examines an extended and comprehensive suite of 27 traditional and 31 technological tools. This level of granularity significantly advances the existing literature, which often focuses on a narrow selection of controls. Moreover, the study adopts a comparative approach by employing the Mann-Whitney U-test to assess differences in perceptions between listed company employees and external auditors. This approach moves the academic discourse beyond single-group surveys toward a rigorous, multi-perspective assessment of control environments. While a perception gap was identified in the traditional tool usage, the consensus between both groups regarding the moderate utilisation of technological tools provides a precise

diagnosis of the technological lag in the corporate sector and offers a comprehensive benchmark for future comparative research in fraud prevention.

Practically, this study's findings provide a strategic roadmap for organisations, regulatory authorities, and professional accountancy organisations across emerging economies. A critical finding of this study is the shared consensus between LC employees and external auditors that fraud is a persistent challenge within the corporate sector. This mutual acknowledgement provides a compelling mandate for capital market regulators to transition from voluntary guidelines toward more stringent enforcement and mandatory compliance frameworks. Moreover, the results highlight a significant perceptual difference regarding traditional tool usage: LC employees perceive a greater reliance on traditional mechanisms than external auditors do. This suggests that management may be overestimating the usage of conventional controls such as bank reconciliations and internal audits. Management should, therefore, prioritise independent control-reality checks to bridge this gap. Furthermore, the findings reveal a critical underutilisation of specialised traditional controls, including whistleblowing policies and dedicated fraud departments. Organisations must formalise these mechanisms to specifically address the ego and *collusion* components of the Fraud Hexagon. Regarding technology-related mechanisms, the study confirms a reactive-tech stance; sophisticated tools such as Benford's Law, digital forensics, and neural networks remain the least utilised despite a high-risk digital environment. Consequently, regulators and professional bodies should move beyond general awareness and implement specific technological guidelines and mandatory training programmes. Enhancing digital literacy and the adoption of software-based analytics is a direct necessity to address emerging fraud patterns that traditional methods are no longer sufficient to capture.

Despite these contributions, the findings of the study should be interpreted considering certain limitations. The population of the study covers professionals only in terms of LC employees and external auditors within a single emerging economy context. Future research could explore cross-country comparisons involving other contexts, thereby obtaining a 360-degree view of fraud risk assessment and control by incorporating perspectives from other stakeholders, including forensic accountants and fraud examiners. Finally, it could be emphasised that strengthening fraud-deterrence mechanisms is crucial for improving transparency and financial integrity within listed companies, particularly in emerging economies where fraud risks continue to evolve.

References

- ACFE (2018). *Report to the nations: 2018 global study on occupational fraud and abuse*. Association of Certified Fraud Examiners. Retrieved on 01 April 2025, from <https://s3-us-west-2.amazonaws.com/acfe-public/2018-report-to-the-nations.pdf>
- ACFE (2020). *Report to the nations: 2020 global study on occupational fraud and abuse*. Association of Certified Fraud Examiners. Retrieved on 01 April 2025, from <https://legacy.acfe.com/report-to-the-nations/2020/>
- ACFE (2022). *Occupational fraud 2022: A report to the nations*. Association of Certified Fraud Examiners. Retrieved on 01 April 2025, from <https://www.acfe.com/-/media/files/acfe/pdfs/rtnn/2022/2022-report-to-the-nations.pdf>
- ACFE (2024). *Occupational fraud 2024: A report to the nations*. Association of Certified Fraud Examiners. Retrieved on 01 April 2025, from <http://www.acfe.com>
- Ali, A. M., Futahi, R. F., Shukur, M. & Al-Orfali, A. K. (2024). Forensic accounting and fraud detection emerging trends and techniques. *Journal of Ecohumanism*, 3(5), 525–542. <https://doi.org/10.62754/joe.v3i5.3921>
- Alleyne, P., & Howard, M. (2005). An exploratory study of auditors' responsibility for fraud detection in Barbados. *Managerial Auditing Journal*, 20(3), 284–303. <https://doi.org/10.1108/02686900510585618>
- Altarraj, M. A. A., & Mokdad, A. (2024). Quantum-assisted machine learning for enhanced fraud detection in cybersecurity. *International Research Journal of Innovations in Engineering and Technology*, 8(5), 319–324. <https://doi.org/10.47001/irjiet/2024.805042>
- Arens, A. A., Elder, R. J., & Beasley, M. S. (2012). *Auditing and assurance services: An integrated approach* (14th ed.). Pearson.
- Arjoon, S. (2005). Corporate governance: An ethical perspective. *Journal of Business Ethics*, 61(4), 343–352. <https://doi.org/10.1007/s10551-005-7888-5>
- Berthet, V. (2022). The impact of cognitive biases on professionals' decision-making: A review of four occupational areas. *Frontiers in Psychology*, 12. <https://doi.org/10.3389/fpsyg.2021.802439>
- Bierstaker, J. L., Brody, R. G., & Pacini, C. (2006). Accountants'

- perceptions regarding fraud detection and prevention methods. *Managerial Auditing Journal*, 21(5), 520–535. <https://doi.org/10.1108/02686900610667283>
- Birol, B. (2019). Corporate governance and fraud detection: A study from Borsa Istanbul. *Eurasian Journal of Business and Management*, 7(1), 44–64. <https://doi.org/10.15604/ejbm.2019.07.01.005>
- CA Sri Lanka (2017). *Code of best practice on corporate governance 2017*. Institute of Chartered Accountants of Sri Lanka.
- Central Bank of Sri Lanka (2023). *Bimpuh Finance PLC - Cancellation of licence issued under the Finance Business Act, No. 42 of 2011*. Retrieved on 28 February 2026, from <https://www.cbsl.gov.lk/en/news/bimpuh-finance-plc-cancellation-of-licence>
- Central Bank of Sri Lanka (2024). *Annual economic review 2023*. Retrieved on 05 April 2025, from <https://www.cbsl.gov.lk>
- Central Bank of Sri Lanka (2025). *Notice to general public on prohibited pyramid schemes*. Retrieved on 28 February 2026, from <https://www.cbsl.gov.lk>
- Central Bank of Sri Lanka (2026). *Notice to the public regarding extension of the administrator of Nation Lanka Finance PLC*. Retrieved on 28 February 2026, from https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/press/notices/notice_20260104_extension_of_the_administrator_of_nation_lanka_finance_e.pdf
- Coderre, D. (2006). *Continuous auditing: Implications for assurance, monitoring, and risk assessment*. The Institute of Internal Auditors. Retrieved on 30 April 2025, from <https://www.qcpa.org.qa/assets/uploads/documents/library/1563184783.pdf>
- Cressey, D. R. (1950). The criminal violation of financial trust. *American Sociological Review*, 15(6), 738–743. <https://doi.org/10.2307/2086606>
- Dissanayake, D. H. S. W., Dissabandara, D. P. P. H., & Ajward, A. R. (2022). An evaluation of the compliance of Sri Lankan listed companies with corporate governance principles and best practices. *Journal of Emerging Financial Markets and Policy*, 1(1), 43–62. <https://doi.org/10.4038/jefmp.v1i1.4>
- Ernst & Young (2018). *15th global fraud survey: Integrity in the spotlight - The future of compliance*. Retrieved on 30 April 2025, from https://giacentre.org/chess_info/uploads/2020/04/EY-15th-Global-Fraud-Survey.pdf

- Farrell, B. R., & Franco, J. R. (1999). The role of the auditor in the prevention and detection of business fraud: SAS No. 82. *Western Criminology Review*, 2(1), retrieved on 08 May 2025, from <http://www.westerncriminology.org/documents/WCR/v02n1/farrell/farrell.html>
- Festinger, L. (1957). *A theory of cognitive dissonance*. Stanford University Press.
- Field, A. (2013). *Discovering statistics using IBM SPSS Statistics: And sex and drugs and rock "n" roll* (4th ed.). Sage.
- Free, C. (2015). Looking through the fraud triangle: A review and call for new directions. *Meditari Accountancy Research*, 23(2), 175–196. <https://doi.org/10.1108/MEDAR-02-2015-0009>
- Freeman, R. E., Dmytriiev, S. D., & Phillips, R. A. (2021). Stakeholder theory and the resource-based view of the firm. *Journal of Management*, 47(7), 1757–1770. <https://doi.org/10.1177/0149206321993576>
- Freeman, R., Wicks, A. & Parmar, B. (2004). Stakeholder theory and “the corporate objective revisited.” *Organization Science*, 15(3), 364–369. <https://doi.org/10.1287/orsc.1040.0066>
- Gill, W. (2009). Fighting fraud with advanced analytics. *Canadian Underwriter*. Retrieved on 05 May 2025, from <https://canadianunderwriter.ca/news/risk/fighting-fraud-with-advanced-analytics/>
- Glover, H. D., & Aono, J. Y. (1995). Changing the model for prevention and detection of fraud. *Managerial Auditing Journal*, 10(5), 3–9. <https://doi.org/10.1108/02686909510087928>
- Grove, H., & Basilico, E. (2008). Fraudulent financial reporting detection: Key ratios plus corporate governance factors. *International Studies of Management & Organization*, 38(3), 10–42. <https://doi.org/10.2753/IMO0020-8825380301>
- 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. <https://doi.org/10.1108/MAJ-02-2015-1163>
- Hall, J. (2011). *Accounting information systems* (7th ed.). Cengage Learning.
- Hillman, A. J., Withers, M. C., & Collins, B. J. (2009). Resource dependence theory: A review. *Journal of Management*, 35(6), 1404–

1427. <https://doi.org/10.1177/0149206309343469>
- Höhne, J. K., & Lenzner, T. (2018). New insights on the cognitive processing of agree/disagree and item-specific questions. *Journal of Survey Statistics and Methodology*, 6(3), 401–417. <https://doi.org/10.1093/jssam/smx028>
- In'airat, M. (2015). The role of corporate governance in fraud reduction: A perception study in the Saudi Arabian business environment. *Journal of Accounting and Finance*, 15(2), 119–128.
- Indrayani, Sukoharsono, E. G., Djamhuri, A., & Roekhudin. (2025). Technological disruption in digital transformation: How should the accounting profession adapt? *Asian Journal of Business and Accounting*, 18(1), 135–167. <https://doi.org/10.22452/ajba.vol18no1.5>
- Jayasinghe, D. T., & Ajward, R. (2019). The level of usage and importance of fraud detection and prevention techniques used in Sri Lankan banking and finance institutions. *CA Journal of Applied Research*, 3, 158–180.
- Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360. [https://doi.org/10.1016/0304-405X\(76\)90026-X](https://doi.org/10.1016/0304-405X(76)90026-X)
- Johnson, G. G., & Rudesill, C. L. (2001). An investigation into fraud prevention and detection of small businesses in the United States: Responsibilities of auditors, managers, and business owners. *Accounting Forum*, 25, 56–78.
- Juhandi, N., Zuhri, S., Fahlevi, M., Noviantoro, R., Nur Abdi, M., & Setiadi, R. (2020). Information technology and corporate governance in fraud prevention. *E3S Web of Conferences*, 202, 16003. <https://doi.org/10.1051/e3sconf/202020216003>
- Kassem, R., & Higson, A. (2012). The new fraud triangle model. *Journal of Emerging Trends in Economics and Management Sciences*, 3(3), 191–195.
- Kassem, R., & Omoteso, K. (2024). Effective methods for detecting fraudulent financial reporting: Practical insights from Big 4 auditors. *Journal of Accounting Literature*, 46(4), 587–610. <https://doi.org/10.1108/JAL-03-2023-0055>
- KPMG (2019). *Global banking fraud survey: The multi-faceted threat of fraud – Are banks up to the challenge?* Retrieved on 25 April

- 2025, from <https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2019/05/global-banking-fraud-survey.pdf>
- KPMG (2023). *A paradigm shift in financial crime: 2023 regulatory challenges*. Retrieved on 25 April 2025, from <https://kpmg.com/xx/en/our-insights/risk-and-regulation/a-paradigm-shift-in-financial-crime.html>
- Law, P. (2011). Corporate governance and no fraud occurrence in organizations: Hong Kong evidence. *Managerial Auditing Journal*, 26(6), 501–518. <https://doi.org/10.1108/02686901111142558>
- Mahathevan, P. (1997). Auditors' use and perception of analytical procedures: Evidence from Singapore. *International Journal of Auditing*, 26(1), 1–18. <https://doi.org/10.1111/1099-1123.00025>
- Malaescu, I., & Sutton, S. G. (2015). The reliance of external auditors on internal audit's use of continuous audit. *Journal of Information Systems*, 29(1), 95–114. <https://doi.org/10.2308/isys-50899>
- Mandal, A., & Amilan, S. (2025). Preventing financial statement fraud in the corporate sector: Insights from auditors. *Journal of Financial Reporting and Accounting*, 23(1), 56–80. <https://doi.org/10.1108/JFRA-02-2023-0101>
- Mangala, D., & Kumari, P. (2017). Auditors' perceptions of the effectiveness of fraud prevention and detection methods. *Indian Journal of Corporate Governance*, 10(2), 118–142. <https://doi.org/10.1177/0974686217738683>
- McKee, T. E. (2006). Increase your fraud auditing effectiveness by being unpredictable!. *Managerial Auditing Journal*, 21(2), 224–231. <https://doi.org/10.1108/02686900610639338>
- Muhammed, R. A., Sushma, C., Harikrishnan, P. R., Kavya, M. K., Bhavana, S., Sanjana, V., & Natesan, G. (2024). Prevention of cyber frauds in the banking sector. *International Scientific Journal of Engineering and Management*, 3(3), 1–5. <https://doi.org/10.55041/isjem01341>
- N'Guilla Sow, A., Basiruddin, R., Mohammad, J., & Abdul Rasid, S. Z. (2018). Fraud prevention in Malaysian small and medium enterprises (SMEs). *Journal of Financial Crime*, 25(2), 499–517. <https://doi.org/10.1108/JFC-05-2017-0049>
- Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature.

Decision Support Systems, 50, 559–569. <https://doi.org/10.1016/j.dss.2010.08.006>

- 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), 15–30.
- Othman, R., Aris, N. A., Mardziah, A., Zainan, N., & Amin, N. M. (2015). Fraud detection and prevention methods in the Malaysian public sector. *Procedia Economics and Finance*, 28, 59–67. [https://doi.org/10.1016/S2212-5671\(15\)01082-5](https://doi.org/10.1016/S2212-5671(15)01082-5)
- Parmar, B. L., Freeman, R. E., Harrison, J. S., Wicks, A. C., Purnell, L., & de Colle, S. (2010). Stakeholder theory: The state of the art. *Academy of Management Annals*, 4(1), 403–445. <https://doi.org/10.5465/19416520.2010.495581>
- Peiris, G. K. H., & Aruppala, W. D. N. (2021). A study on fraud prevention and detection methods in Sri Lanka. *Kelaniya Journal of Management*, 10(2), 37–56. <https://doi.org/10.4038/kjm.v10i2.7692>
- Phua, C., Lee, V., Smith, K., & Gaylar, R. (2010). A comprehensive survey of data mining-based fraud detection research. *Artificial Intelligence Review*.
- Rahman, M. J., & Jie, X. (2024). Fraud detection using fraud triangle theory: Evidence from China. *Journal of Financial Crime*, 31(1), 101–118. <https://doi.org/10.1108/JFC-09-2022-0219>
- Rahman, R. A., & Anwar, I. S. K. (2014). Effectiveness of fraud prevention and detection techniques in Malaysian Islamic banks. *Procedia – Social and Behavioral Sciences*, 145, 97–102. <https://doi.org/10.1016/j.sbspro.2014.06.015>
- Ramesh, R., & Vinayagathan, T. (2024). The impact of corruption, rule of law, accountability, and government expenditure on government effectiveness: Evidence from Sri Lanka. *Journal of Asian and African Studies*, 59(6), 1843–1866. <https://doi.org/10.1177/00219096221146999>
- Rao, T. V. N., Darapu, K., & Marukukula, M. (2025). Fraud detection and prevention in finance and banking using artificial intelligence. In S. Mallik, S. Mathivanan, S. Sangeetha, & B. Soufiene (Eds.), *Real-world applications of AI innovation* (pp. 213–232). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-4252-7.ch011>

- Rathnasiri, U. A. H. A., & Bandara, R. M. S. (2017). The forensic accounting in Sri Lanka: Perception of professional accountants. *Kelaniya Journal of Management*, 6(2), 68–82. <https://doi.org/10.4038/kjm.v6i2.7546>
- Rostami, V., & Rezaei, L. (2021). Corporate governance and fraudulent financial reporting. *Journal of Financial Crime*. 29(3), 1009–1026. <https://doi.org/10.1108/JFC-07-2021-0160>
- Rustiarini, N. W., & Sunarsih, N. M. (2017). Factors influencing the whistleblowing behaviour: A perspective from the theory of planned behaviour. *Asian Journal of Business and Accounting*, 10(2), 187–214
- Siegel, S., & Castellan, N. J. (1988). *Nonparametric statistics for the behavioral sciences* (2nd ed.). McGraw-Hill.
- Tajfel, H., & Turner, J. C. (1979). An integrative theory of intergroup conflict. In W. G. Austin & S. Worchel (Eds.), *The social psychology of intergroup relations* (pp. 33–47). Monterey, CA: Brooks/Cole.
- Tan, K., Liu, Y., & Ye, Q. (2023). A gendered discourse on truthful disclosure of financial fraud practices among accountants in China. *Accounting Research Journal*, 36(2–3), 230–250. <https://doi.org/10.1108/ARJ-07-2022-0160>
- Tum, K. (2013). Continuous audit: From the concept towards the implementation. *International Journal of Business and Social Research*, 3(7), 1–7.
- Uecker, W. C., Brief, A. P., & Kinney, W. R. (1981). Perception of the internal and external auditor as a deterrent to corporate irregularities. *The Accounting Review*, 56(3), 465–478. <http://www.jstor.org/stable/246909>
- Vousinas, G. L. (2019). Advancing theory of fraud: The S.C.O.R.E. model. *Journal of Financial Crime*, 26(1), 372–381. <https://doi.org/10.1108/JFC-12-2017-0128>
- Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *CPA Journal*, 74(12), 38–42.
- World Bank (2024). *Sri Lanka development update: Opening up to the future*. Retrieved on 25 June 2025, from <https://www.worldbank.org/en/country/srilanka/publication/sri-lanka-development-update-2024>
- Zhou, W., & Kapoor, G. (2011). Detecting evolutionary financial statement fraud. *Decision Support Systems*, 50, 570–575. <https://doi.org/10.1016/j.dss.2010.08.007>