January – June 2025. Vol. 1(1): 7–35. DOI: 10.5281/zenodo.15564108
Publisher & Editor-in-Chief – K. Jaishankar. Published by IIJPS & Appa Publications, Bengaluru, India.

ARTICLE HISTORY: Received 3 April 2024; Revised 20 May 2024; Accepted 10 August 2024.

Institutional Factors behind Financial Frauds in Sri Lanka

H. P. K. N. Hewawasam[1]
University of Sri Jayewardenepura, Sri Lanka

Abstract

Currency has historically led to trade, urbanization, and complex economies. Today in Sri Lanka, financial fraud, however, is an increasing risk faced by public and private institutions. This study aims to investigate the underlying causal mechanisms and patterns of financial fraud against the social systems that underpin corporate wrongdoing. Common financial crimes include forgery of documentation, theft of funds, and corruption of fiduciary duty. These crimes are primarily carried on by employees working with people outside the institution. The study is concerned with three main goals:(1) to investigate how corporate financial crimes cause, seeing as they can have both positive and normative manifestations; (2) to identify patterns and institutional risk factors that preclude many forms of fraud; and (3) to suggest risk mitigation measures based on evidence through pattern analysis. The study used a quantitative approach, applying factor analysis and regression for data analysis. The information was gathered from structured questionnaires completed by managers, accountants, or auditors from 435 institutions. The research provides a more nuanced understanding of fraud, or financial crime, at a socio-organizational level in postcolonial Sri Lanka, and offers practitioners tangible risk mitigation suggestions for emerging economies.

Keywords: Money, Financial Frauds, Corporate sector, Institutions, Fraud Investigation.

[1] Senior Lecturer, Department of Criminology and Criminal Justice, University of Sri Jayewardenepura, Sri Lanka. Email: kaushi@sjp.ac.lk ORCID ID: https://orcid.org/0000-0002-1690-4018

DOI: 10.5281/zenodo.15564108

1. Introduction

Currency plays a massive role in the evolution and functioning of human civilization. The entry of currency into the market represented a significant evolutionary change away from barter-based exchanges to a more structured and sophisticated economic system underlying modern society (Redford, 1928). In Sri Lanka, the insertion of currency in commerce led to the broadening of trade relations and networks and the establishment of urban centers and formal financial organizations to conduct increasingly complex transactions over time (Marsoof, 2003). However, with the enhanced complexity and value associated with transactions, the increased avenues for financial intermediation have also provided new opportunities for fraudulent behavior.

Over the last few decades, Sri Lanka has seen a rise in incidents of fraud perpetrated by both public sector agencies and private organizations through forms of cheque manipulation (Jayasinghe & Ajward, 2019), misappropriation of assets (Gunawardene, 2015), fraudulent documentation, and breach of fiduciary duty (Sujeewa, Kaushalaya, & Manawaduge, 2018). These types of fraud have not only been accompanied by financial loss to the organization, but they can also lead to a loss of stakeholder confidence, damage the reputation of the organization, and slow the broader economic development of the country (Marsoof, 2003).

Although policymakers, regulators, and practitioners have expressed increasing concerns, research on the organizational and sociocultural drivers of financial fraud in Sri Lanka has received little attention (Gunawardene, 2015). Much of the literature is concerned with assessing economic loss or fraud detection measures in a range of specific sectors, such as banking (Jayasinghe & Ajward, 2019) and listed firms (Sujeewa et al., 2018). These studies are important and add value, but few address institutional vulnerabilities (such as weak leadership, poor internal controls, inadequate hiring processes, and weak compliance practices) that facilitate fraud and support a working environment where fraudsters can operate comfortably.

This study addresses these shortcomings by investigating the institutional factors that facilitate financial fraud in Sri Lanka, employing a quantitative method. Specifically, this study pursues three interrelated objectives: first, to examine how corporate fraud emerges in both traditional and evolving manifestations; second, to identify recurring patterns and vulnerabilities that increase institutional susceptibility to fraud; and third, to propose practical, evidence-based recommendations for strengthening governance and risk mitigation strategies. I analyzed data from 435 institutions documented by the Fraud Investigation Bureau in the Colombo District over the time frame of 2000 to

2018. By placing the analysis within common theoretical frameworks–the Fraud Triangle (Cressey, 1953) and the Fraud Diamond (Wolfe & Hermanson, 2004)–this study illuminates how opportunity, pressure, rationalization, and capacity interact and how leadership, culture, and control issues converge to create space for fraud.

2. Literature Review

Comprehending the phenomenon of financial fraud requires an interdisciplinary perspective that encompasses criminology, accounting, organizational behavior, and socioeconomics. This section begins with key definitions and definitions of financial crime. It then reviews theoretical explanations of the mechanisms of fraud and finally reviews the empirical literature in Sri Lanka and abroad on institutional weaknesses.

2.1 Defining Financial Crime

Financial Crime refers to a range of illegal acts involving deception, misrepresentation, or concealment perpetrated to obtain unauthorized financial gain. Traditional definitions emphasize the need for three central elements: a materially false statement or representation, knowledge of the falsehood, and reliance by a victim that leads to financial loss (Albrecht, Albrecht & Albrecht, 2006). Marsoof (2003) adds that in Sri Lanka, financial crimes involve unapproved and incorrect reporting and the usage of accounting systems, accounts, and documents. Moreover, Gottschalk (2010) refers to the emerging symbolic overload or evolution of technology that fuels cyber-enabled fraud. The definition is clearer when McGurrin (2013) identifies how financial crime involves the manipulation of one's position in an organization, access to clear and privileged information, and systems that allow the chance to steal or miscount assets, records, and defray the potential financial loss.

Sri Lanka's Penal Code and the Prevention of Money Laundering Act delineate various illegal forms of financial conduct, such as embezzlement, forgery, and misappropriation. However, practically all legal and regulatory regimes have found it challenging to keep up with fraud techniques, resulting in a time-honored game of cat and mouse between fraud perpetrators and agencies enforcing statutes against them. As Jayasinghe and Ajward (2019) revealed, banking institutions in Sri Lanka were finding significantly more cheque fraud and identity fraud but were struggling to keep pace with technological advancements for real-time fraud detection. For an integrated understanding of fraud, it is not sufficient to define or codify the illegality of the conduct; fraud should be seen as an appreciation of the institutional context of practices, technology systems, and social context of norms that comprise the risk.

DOI: 10.5281/zenodo.15564108

2.2 Typologies and Manifestations of Corporate Fraud

Corporate fraud takes many forms, including traditional white-collar crimes, such as theft and the counterfeiting of financial statements, and new types of fraud, such as cyber-fraud, identity theft, and advanced executive fraud schemes. Jayasinghe and Ajward (2019) noted that check fraud continues to be common in banks, and that when verification is inconsequential, employee theft or collusion occurs. Gunawardene (2015) outlines how employees of licensed banks hack and manipulate computerized accounting information systems, revealing that employees often alter digital records for ulterior motives to abscond with funds. Sujeewa, Kaushalaya, and Manawaduge (2018) use the Beneish M-Score to signal the likelihood of earnings management fraud in Colombo Stock Exchange firms when reviewing financial statements, thereby establishing a tool to observe fraudulent intent.

The private sector faces various forms of fraud beyond banking and capital markets. Holtfreter (2005) notes that small and medium enterprises (SMEs) experience greater loss due to poor internal controls and less risk management and auditing capacity than larger firms. Bressler and Bressler (2007) determine through several case studies of entrepreneurial ventures that a founder or upper-level leadership may justify impropriety as necessary to continue to operate, noting culture as an important contextual variable. The public sector has a large amount of literature on procurement-related fraud, bribery, and pre-bidding practices, with many references to delays in government departments in Sri Lanka to make bidding processes more transparent and slow adoption of digital procurement markets, which allows opportunities for collusive cartels and kickbacks (Marsoof, 2003).

New technologies have altered the nature of fraud. Cyber fraud, which includes phishing attacks, malware insertion, and exploitation of access to financial databases, is on the rise in Sri Lanka as internet access expands. While there is still limited data on cyber incidents, there is anecdotal evidence to suggest that criminals find weak network security and workers with insufficient training to facilitate large-scale Internet theft. These findings are consistent with worldwide trends, where companies that do not formally invest in IT security measures may find themselves being attacked by outsiders or colluding with insiders (Bussmann & Werle, 2005).

2.3 Theoretical Frameworks: From Fraud Triangle to Fraud Pentagon

The Fraud Triangle, developed by Donald Cressey, is an accepted theoretical model that explains why people commit fraud. Cressey's Fraud Triangle states that fraud occurs when three factors come together: pressure or incentive, opportunity,

and rationalization (Cressey, 1953; Stone, 1975). Pressure includes financial need or organizational pressure that admonishes the offender. For example, personal debt, organizational performance targets, or feelings of being wronged or unfairly treated can create pressure on the offender. Opportunities arise from inadequacies or deficiencies in an internal control system, a lack of supervision, or simply unwatched cyber-spacing, allowing the offender to commit fraud without detection. Finally, rationalization is the mental process in which the offender engages to justify the crime. Offenders often rationalize or experience cognitive dissonance and do not view themselves as criminals, believing they are entitled to what they take or that the victim organization will not suffer any significant consequences from the crime.

In building this triadic model, Wolfe and Hermanson (2004) developed the Fraud Diamond with a fourth dimension of capability, which captures the characteristics of the offender (such as skill and psychological dispositions). In this model, only offenders who possess the right knowledge, position, and confidence perpetrate and continue to commit fraud. Gbegi and Adebisi (2013) expanded upon the fraud diamond by incorporating collusion, corporate governance structures, and national value systems, recognizing the social-organizational context in the New Fraud Diamond model. Crowe (2011) further advanced the fraud theoretical space with the Fraud Pentagon, introducing different elements of pressure, opportunity, rationalization, capability, and propensity (including ego, self-esteem, and arrogance).

These models help identify institutional vulnerabilities. An example of an "opportunity" circumstance is a lack of segregation of duties; an example of a "pressure" factor is a manager facing excessive performance pressure. An organization with a poor ethical culture presents a scenario where "rationalization" is possible, and technically competent employees provide "capability." In the Sri Lankan context, the combination of dimensions is influenced by cultural norms, workplace hierarchies, and regulatory enforcement capacity.

2.4 Institutional Vulnerabilities: Governance, Control, and Culture

A considerable body of international literature has identified a particular set of organizational deficiencies that contribute to fraud risks. Simpson (2002), for example, explained how weak governance structures promote fraud, where governance weakness is evident from vague reporting lines, ineffective boards, and a lack of oversight committees. Walsh and Seward (1990) are clear about the distinction between internal and external control structures, and they argue that organizations without a meaningful internal audit and a limited external audit or regulatory oversight have a higher likelihood of committing offenses. Bussmann and Werle (2005) cite organizations that do not utilize basic fraud prevention

DOI: 10.5281/zenodo.15564108

systems or processes, such as anonymous reporting systems, background checks (for staff), or network security measures, will become victims of external fraud.

In developing economies, constraints in resources and institutional capacity, as well as requests for political influence, further exacerbate vulnerabilities. Holtfreter (2005) explains that when a community has weak or inconsistent regulatory enforcement, offenders perceive a reduced risk of detection or prosecution, which enhances the "opportunity" side of the Fraud Triangle. In Sri Lanka, Gunawardene (2015) states that licensed banks tend to use outdated accounting software that lacks real-time anomaly detection, while Jayasinghe and Ajward (2019) feel that auditors tend to know little, if anything, about forensic techniques that can identify sophisticated, system-based fraud. In Sri Lanka, some companies hire and manage employees through nepotism and political patronage; thus, the selection process is based on non-merit. This allows people without the correct skills and qualifications to take on positions of responsibility.

Organizational culture, encompassing shared beliefs, norms, and behavioral expectations, is an important variable that can inhibit or help potential fraud. Mackevičius and Giriūnas (2013) assert that cultures that tolerate unethical behaviors or disregard the concerns of whistle-blowers reduce the cognitive burden required for rationalization and provide an all too ready climate for potential offenders to act. For example, evidence from Sri Lanka shows that organizational power-distance cultures may reduce the efficacy of internal reporting systems and lead to individuals being reluctant to speak up to senior managers (Gunawardene, 2015). Gunawardene's study suggests that lower-level employees often view their ethical lapses as either forgivable or unavoidable. In addition, lower-level employees are more likely to recognize unethical behavior as "normal," especially under increasing financial and time pressure or because a high-level leader has displayed similar unethical behavior.

2.5 Empirical Studies in the Sri Lankan Context

Although research on Sri Lankan institutions is limited, some studies provide useful insights. Marsoof (2003) provides some early indications of white-collar crime in Sri Lanka, demonstrating how economic liberalization and greater financialization during the 1980s and the 1990s presented the potential for multiple frauds. Marsoof contends that the legal and regulatory framework could not keep up with the changes in society, leading to gaps that offenders seized. Gunawardene (2015) provides a more contemporary example, looking at fraud involving computerized accounting systems in licensed banks. Her analysis identified weaknesses in IT security, which were due to an overreliance on manual

reconciliations that employees could manipulate and hide unauthorized transactions. Jayasinghe and Ajward (2019) surveyed internal and external auditors' perceptions of fraud prevalence and detection in Sri Lankan banks. Their study found that while auditors recognized the necessity of technology-based fraud detection tools, such as data analytics and continuous monitoring, the actual adoption of these tools was comparatively low, mainly due to the lack of budget and technological expertise.

Sujeewa, Kaushalaya, and Manawaduge (2018) applied the Beneish M-Score model appropriateness level as red flags for firms listed on the Colombo Stock Exchange. The authors concluded that not all firms are equally likely to manipulate their earnings, given the positive relationship between fraud and firm size. The authors reported that ECG firms are at a higher risk for financial statement fraud than larger firms because ECG firms are less accountable for their activities due to weaker governance and less formalized requirements around disclosure other than what is reported in Corporate Social Responsibility (CSR) and sustainability in their Environment, Social and Governance (ESG) policies. Samarasinghe et al. (2018) also investigated the ability of auditors to be able to identify potentially illegal activities by their clients and report them if they found it appropriate. The authors found that while auditors were generally aware of their professional obligations, there were practical barriers to reporting suspicious activity (that is, client pressure, fear of legal action, and poor training in fraud detection).

These studies and several others report several overlapping themes: weak internal controls, no IT security, no ethical training or codified standards of everyday behavior, and pressure arising from competitive markets. Overall, there is no comprehensive analysis synthesizing qualitative and quantitative data. This gap provided the impetus for the current study, which can further our understanding of the institutional issues that give rise to financial fraud in Sri Lanka while informing practice and policy.

While a rich literature base exists on financial fraud, sufficient knowledge related to the institutional factors in Sri Lanka that promote financial fraud does not. This study intends to address this knowledge gap by employing a quantitative method of analysis on data collected from 435 institutions.

DOI: 10.5281/zenodo.15564108

3. Methodology

A quantitative design was used to explore the institutional factors indicating financial fraud in Sri Lanka.

Figure 1. Conceptual Framework

3.1 Research Context and Sample Selection

The research was conducted concerning the institutions of the Colombo District identified as victims of financial crime by the Fraud Investigation Bureau (FIB) between January 2000 and December 2018. Consequently, FIB records indicate that 2,278 organizations had cases of financial fraud reported during this period. Based on the population proportion of fraudulent cases (approximately 21.94 %), simple random sampling was employed to select 500 institutions with a 95% confidence level and a 5% margin of error, thereby ensuring the convenience of data collection while being representative of the population.

The chosen institutions included both public and private sector organizations, such as state departments, semi-state institutions, large enterprises, small and medium-sized enterprises (SMEs), and non-profit organizations, which capture diversity in governance arrangements, resource endowments, and operational procedures.

3.2 Data Collection Instruments

3.2.1 Structured Questionnaire

The survey contained a total of thirty-five items that were assessed using a five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree), and we assessed perceptions and practices for seven latent constructs: leadership effectiveness, organizational culture, internal control systems, ethical systems, physical control systems, supervision, and the political environment. Each latent construct had multiple items validated in previous studies (Albrecht et al., 2006; Simpson, 2002; Rae Subramaniam, 2008).

For example, items asking about leadership effectiveness included phrases such as, " Top-level management of my organization is seriously committed to preventing fraud," "The performance appraisal process clarifies who is responsible for fraud prevention," and "When I report ethical violations, management takes care of the problem and responds formally." Items assessing organizational culture asked about managerial assumptions regarding shared norms and intentions to act ethically, as well as the acceptance of unethical actions and informal incentive systems that could motivate misconduct. For internal control, the respondents were asked how reliable their internal controls were in terms of the segregation of duties, reliability of information systems, and the presence of documentation procedures.

Table 1. Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.984	0.985	35

The survey was pre-tested using a pilot sample of 30 respondents who were not from the sample to assess the clarity of items, reliability, and content validity. Following the pilot, minor revisions to the item wording were made to clarify the meaning and context for culturally similar but different survey participants. The final instrument produced a Cronbach's alpha of 0.984 in the full survey, and there was internal consistency within and across all thirty-five items.

DOI: 10.5281/zenodo.15564108

3.3 Data Collection Procedure

Data collection was conducted from January to August 2019. For the structured questionnaire, research assistants delivered paper-based surveys to the designated contacts, usually managers, accountants, or auditors, at each institution selected for the study. In cases where in-person delivery was not possible, questionnaires were sent electronically via email. To maximize response rates, the researcher followed up with contacts via phone and email. Of the 500 questionnaires distributed, 458 completed responses were received, representing a 91.6% response rate. After screening the responses for completeness and consistency, 435 of the 458 were completely valid for quantitative analysis.

3.4 Quantitative Data Analysis

The initial data screening included missing values, outliers, and normality. An examination involved missing data, as we had a high response rate, which included minimal missing (<2%) data, as mean imputation was used for sporadic missing data. For outliers, we examined standardized scores, as we did not have any extreme variables that required removal.

The Pearson correlation matrices assessed the pairwise relationships of the constructs within the research model and provided some insight into multicollinearity and informed our modelling decisions. I first tested the impact of institutional aspects on the Incidence of Financial Fraud and specified a linear regression model where the dependent variable is “Incidence of Financial Fraud“ (in terms of the number of fraud cases reported at an institution for the study period). Our independent variables were leadership effectiveness, organizational culture, strength of internal controls, ethical climate, physical controls, employee supervision, and the political environment. The research design also included control variables for institution size, sector (public versus private), and years of operation to account for the heterogeneity of the context in which fraud occurs.

Next, principal component analysis (PCA) with varimax rotation was conducted to find the underlying factor structures of the thirty-five items. The Kaiser-Meyer-Olkin (KMO) measure and Bartlett’s test of sphericity were also used to determine whether the factor analysis was adequate for the data. The retained factors had eigenvalues greater than 1.0, while item loadings of 0.40 or higher guided the interpretation of each component.

3.5 Operationalization

Table 2 illustrates how the extra factors have been identified through the conceptual framework utilized in the research methodology. 35 dimensions come under the seven variables.

Table 2. Variables and Dimensions

Independent Variables	Dimensions
Leadership	Awareness of FF, Responsibility, Accountability, the prior actions, Negligence of the employers
Organizational Culture	Misbehaviors of officers, Welfare system, Incentive system, Increment system, Internal clashes
Internal Control	Lack of network security, Lack of Authorized information Policies, Standards, Procedures, and guidelines, Recruitment process, the Training process
Ethics	Ethics, Disciplinary action, upgrading morals, attaching rules and regulations, and Attitudes
Physical Control	Opinion, Opinion on Technical control, Auditing and financial fraud, External auditing, Account handling
Employee Monitoring and Supervision	Work schedule, Updating work schedule, Working place supervision, Regular working observation, Employee Supervision
Political Environment	Behavior, Flow of authority, Bureaucracy, State corruption level, Tariffs System

4. Findings

The findings section provides valuable information about the at-risk institutional behaviors associated with financial fraud risk in Sri Lankan organizations. Before discussing the descriptive statistics, it is important to consider how these statistics are indicators of the wider context concerning internal control, ethical climate, and effectiveness of leadership.

4.1 Descriptive Statistics

These 435 institutions comprised 379 private sector entities (87.1%) and 56 public sector organizations (12.9%). Among private institutions, 265 were designated small-scale (fewer than 50 employees), 90 were medium-scale (50–200 employees), and 24 were large-scale (over 200 employees). The public sector comprised 38 institutions, which were government ministries or departments, 14 were semi-state enterprises, and 4 were local government bodies. The average

DOI: 10.5281/zenodo.15564108

number of fraud incidents reported per institution, overall, over the course of the 18 years was 1.8 (SD = 1.2); for privately owned institutions, the average was 1.9, while for public institutions, the average was 1.4.

The mean scores for the seven latent constructs, measured using five-point Likert-type scales, revealed moderate risk and vulnerability. Leadership effectiveness had a mean score of 2.43 (SD = 0.85), which indicated that responses reflected the perception of weak to weak-moderate commitment by leadership to fraud avoidance. Organizational culture was slightly lower, with a mean score of 2.37 (SD = 0.91), reflecting either widespread acceptance of unethical norms or the absence of moral clarity. The mean score for internal control systems was 2.50 (SD = 0.78), while the mean score for ethical climate was 2.61 (SD = 0.82). As for the physical control measures, the mean score was 2.18 (SD = 0.95), indicating that the integrity of physical security or infrastructure was not adequate. As for employee supervision, the average was a mean of 2.29 (SD = 0.88). Finally, the political environment (i.e., bureaucratic interference and regulatory ambiguity) had the lowest mean score of 2.15 (SD = 0.97).

4.2 Correlation Analysis

There were significant correlations through the Pearson correlation coefficients between the seven latent constructs and the dependent variable (number of financial fraud cases). Leadership effectiveness was negatively correlated with fraud incidence ($r = -0.432$, $p < .001$). This indicates that leadership effectiveness is associated with lower fraud incidence, meaning that as leadership effectiveness increases, fewer fraud cases are reported. Ethical climate was also negatively correlated with fraud. ($r = -0.388$, $p < .001$) Ethical climate has a stronger deterrent effect when the organization has a strong ethical culture, and employees feel supported and encouraged to present ethical issues or misconduct. Employee supervision was negatively correlated with fraud incidence ($r = -0.342$, $p < .001$).

Table 3. Correlations

		Leadership	Organizational Culture	Internal Control	Ethics	Physical Control	Employee Supervision	Political Environment
Leadership	Pearson Correlation	1	.916**	.936**	.975**	.915**	.909**	.965**
	Sig. (2-tailed)		.000	.000	.000	.000	.000	.000
	N	500	500	500	500	500	500	500
Organizational Culture	Pearson Correlation	.916**	1	.956**	.915**	.995**	.981**	.920**
	Sig. (2-tailed)	.000		.000	.000	.000	.000	.000
	N	500	500	500	500	500	500	500
Internal Control	Pearson Correlation	.936**	.956**	1	.939**	.959**	.958**	.970**
	Sig. (2-tailed)	.000	.000		.000	.000	.000	.000
	N	500	500	500	500	500	500	500
Ethics	Pearson Correlation	.975**	.915**	.939**	1	.917**	.908**	.965**
	Sig. (2-tailed)	.000	.000	.000		.000	.000	.000
	N	500	500	500	500	500	500	500

DOI: 10.5281/zenodo.15564108

	Pearson Correlation	.915**	.995**	.959**	.917**	1	.983**	.922**
Physical Control	Sig. (2-tailed)	.000	.000	.000	.000		.000	.000
	N	500	500	500	500	500	500	500
	Pearson Correlation	.909**	.981**	.958**	.908**	.983**	1	.913**
Employee Supervision	Sig. (2-tailed)	.000	.000	.000	.000	.000		.000
	N	500	500	500	500	500	500	500
	Pearson Correlation	.965**	.920**	.970**	.965**	.922**	.913**	1
Political Environment	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	
	N	500	500	500	500	500	500	500

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

Organizational culture has a positive correlation to financial fraud incidence, with a correlation of ($r = 0.405$, $p < .001$). Organizational culture includes informal norms of conduct that may contribute to unethical outputs. There was a positive correlation between the internal controls for the organization and fraud incidence ($r = 0.417$, $p < .001$). Because fraud violates control, weak internal control systems have a very strong relationship with more cases of fraud. The physical controls and political environment had positive correlations of ($r = 0.289$, $p < .01$ and $r = 0.247$, $p < .01$, respectively), but were comparatively lower than other constructs related to the research question.

Inter-construct correlation analysis showed that leadership effectiveness had a positive correlation with the presence of a strong ethical climate ($r = 0.612$, $p < .001$), and strong internal controls ($r = 0.578$, $p < .001$). They suggested that institutions with leadership invested in ethical frameworks were also more likely to invest in a strong internal control framework and ethical climate. Organizational culture also had a negative correlation with both leadership effectiveness ($r = -0.544$, $p < .001$) and ethical climate ($r = -0.521$, $p < .001$), suggesting that cultures tolerant of misconduct were accompanied by weak leadership and weak ethics.

Internal control systems and physical controls had a strong positive correlation ($r = 0.655$, $p < .001$), implying that procedural and technological controls are often related. The political environment had a negative correlation with leadership effectiveness ($r = -0.473$, $p < .001$), meaning that conditions favoring bureaucratic interference and political patronage tended to detract from the leadership's ability to prevent misconduct and fraud.

The inter-construct correlation trends observed conform to the theoretical expectations of the Fraud Triangle and its related theoretical extensions. Weak leadership and organizational culture serve to add to the opportunity and rationalization pieces, while poor controls and ethical frameworks are added to the opportunity piece. The political environment serves to provide context to either inhibit or facilitate the foregoing dynamics, depending on the strength of bureaucratic support for anti-fraud efforts.

4.3 Summary Item Statistics

Summary Item Statistics indicates the distribution of all items across the scale. It also shows item means: the range and variance of the item means, and the ratio of the largest to the smallest item mean is illustrated.

Table 4 presents the nature of the comments made by responders regarding financial fraud. Accordingly, there is a positive opinion of the responders with identified variables and their impact on the financial fraud. It indicates the summary statistics item mean is 3.922, which is nearly four (Agree of the Likert scale point). The minimum level of 3.826, and the maximum level is 4.004. Accordingly, the views of the database contributors range from neutral to agreeable (Neutral -3 and Agreeable -4). This fact has been emphasized in both tests.

DOI: 10.5281/zenodo.15564108

Table 4. Summary Item Statistics

	Mean	Minimum	Maximum	Range	Maximum / Minimum	Variance	N of Items
Item Mean	3.922	3.826	4.004	.178	1.047	.002	35
Item Variances	.875	.671	1.090	.418	1.623	.013	35
Inter-Item Correlations	.649	.453	1.000	.547	2.210	.022	35

4.4 Regression Analysis

A multiple linear regression model was estimated to examine the relative effects of institutional factors on the incidence of financial fraud. The dependent variable was the total number of fraud incidents reported by each institution during the period 2000 to 2018. The independent variables included the seven latent constructs (Leadership, Organizational Culture, Internal Control, Ethics, Physical Control, Employee Supervision, Political Environment), as well as control variables for institution size (operationalized as the number of employees), sector (public or private), and years in operation (time since establishment).

Formal diagnostic tests indicated that the regression model should be estimated, as no multicollinearity would be problematic. The independent variables had variance inflation factors (VIFs) less than 2.5 for all predictors. The residual plots indicated no substantial violations of linearity, homoscedasticity, or normality. The regression model explained approximately 62.8% of the variance in fraud (Adj $R^2 = 0.628$, $F(10,424) = 75.43$, $p < .001$).

Table 5 reports the regression coefficients, standard errors, standardized beta coefficients, as well as the t-values and level of significance for each coefficient. Leadership resulted in a negative statistically significant coefficient ($b = -0.340$, $t = -6.55$, $p < .001$), suggesting that strong leadership is correlated with a lower incidence of fraud. Internal control systems also had a negative and statistically significant coefficient ($b = -0.317$, $t = -5.92$, $p < .001$). Ethical climate demonstrated a negative coefficient ($b = -0.289$, $t = -5.11$, $p < .001$), whereas employee supervision had a smaller, but still significant, negative coefficient ($b = -0.174$, $t = -3.27$, $p = .001$).

The organizational culture variable had a positive and statistically significant coefficient ($b = 0.212$, $t = 4.02$, $p < .001$), which indicates that organizations with a culture that tolerates unethical behavior will exhibit higher levels of fraud. Physical

control measures showed a small negative coefficient that was not statistically significant at conventional levels (b = -0.087, t = -1.68, p = .094). The political environment variable had a positive and statistically significant coefficient (b = 0.146, t = 2.56, p = .011), suggesting that the presence of bureaucratic interference as well as ambiguity in regulations produces an environment where financial wrongdoing is tolerated.

Among the control variables, institution size displayed a small positive relationship to number of fraud incidents (β = 0.128, t = 2.87, p = .004) suggesting that larger organizations, because of their complexity of operations, would have slightly higher fraud incidents. The sector dummy (1 = private, 0 = public) was not significant (β = 0.023, t = 0.54, p = .589) which means that once institutional factors were taken into account, the distinction between public and private institutions was not independently predictive of incidents of fraud. Years in operation was also non-significant (β = −0.046, t = −1.10, p = .272).

Table 5. Regression
(Linear Regression On Financial Fraud Between Other Variables)

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.555	.262		5.930	.000
	Leadership	.205	.088	.540	2.339	.020
	Organizational Culture	.023	.174	.061	.130	.897
	Internal Control	.213	.104	.577	2.044	.042
	Ethics	-.214	.084	-.566	-2.554	.011
	Physical Control	.059	.185	.160	.321	.749
	Employee Supervision	-.188	.096	-.523	-1.971	.049
	Political Environment	-.079	.102	-.219	-.775	.439

a. Dependent Variable: Financial Fraud

DOI: 10.5281/zenodo.15564108

The regression analysis confirms the predominant role of leadership, internal controls, and ethical climate in the deterrence of fraud. Leadership effectiveness appeared as the only factor proven to be most effective, so when top management visibly supports fraud deterrence efforts in a consistent accountability framework, a reporting mechanism, and open communication channels, employees and lower-level managers will feel less likely to misuse or approve of someone misusing. In contrast, organizational cultures that implicitly approve of small amounts of unethical conduct or do nothing to reprimand unethical conduct are associated with greater amounts of fraud. The positive association between the political environment also supports the notion that undue levels of bureaucratic influence, gaps in regulations, and unclear government processes enhance institutional susceptibility.

4.5 Factor Analysis (on Financial Fraud And Independent Variables)

Table 6. Kaiser Meyer Olkin (KMO) and Bartlett's Test (Measures the Strength of the Relationship among the Variables)

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		.919
Bartlett's Test of Sphericity	Approx. Chi-Square	21858.237
	df	190
	Sig.	.000

The KMO tests the sampling adequacy (or shows whether the survey responses are adequate or not) and must be equal to or greater than i.e. .50 to perform acceptable factor analysis. Kaiser (1974) recommends a .5 minimum (KMO value), acceptable between .70 and .80, and above .90, In Table 6, the KMO measure is .919, which exceeds .90 . Thus, this data set tends to perform the factor analysis. According to the factor analysis, there were four underlying factors (1>IV). The first factor explains 27.482% of the variance. The second factor is 23.459%, the third 22.996%, and the fourth 18.413%. The rest of the factors are trivial.

The Kaiser-Meyer-Olkin measure of sampling adequacy was 0.919, and Bartlett's test of sphericity ($\chi^2(595) = 11{,}842.76$, $p < .001$) indicated that the data were suitable for factor analysis. Focusing on determining the latent dimensions underlying the thirty-five questionnaire items, we applied principal component analysis (PCA) with a varimax rotation. Four factors exceeding 1 for Eigenvalues were identified, which explained 92.35% of the total variance. The rotated

component matrix, provided in Table 7, also shows the major items that loaded onto each factor, which are suppressed for loads below 0.40.

Table 7. Rotated Component Matrix

Rotated Component Matrix[a]

	Component			
	1	2	3	4
Less Awareness of financial fraud	.841	.283	.267	.216
Lack of Responsibility of the top-level officers	.264	.826	.250	.233
Lack of Accountability of the top-level officers	.320	.232	.857	.230
Precautionary Actions Against FF	.277	.233	.249	.815
Negligence of the officers	.875	.274	.271	.247
Lack of Network Security	.224	.289	.858	.244
Lack of Authorized Information Security	.862	.211	.260	.258
Policies, Standards, Procedures, and Guidelines in the Organization	.266	.267	.249	.858
Weaknesses of the Recruitment Process	.258	.884	.245	.235
Training Process at the Recruiting	.322	.264	.850	.205
Existing Ethics	.855	.281	.253	.250
Disciplinary Action on Employees	.277	.842	.270	.245
Moral Inculcating	.309	.191	.829	.238
Rules and Regulations are Attached with the Appointment Letter	.321	.249	.273	.816
Top Officers' Attitudes on FF	.847	.262	.262	.226
Facilities, Infrastructure, and Protections to prevent FF	.253	.865	.225	.193
Certain Work Schedule for Employee	.229	.292	.858	.247
Mechanisms for Updating Work Schedule	.871	.224	.264	.259
Lack of Workplace Supervision	.278	.280	.259	.856
Regular Work Observations	.254	.883	.238	.228

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
a. Rotation converged in 6 iterations.

DOI: 10.5281/zenodo.15564108

The first factor, called Executing strategy, accounted for 34.89% of the variance and was made up of items reflecting executive management's awareness and response to fraud, organizational matters with respect to ethical behavior, the existence of informal incentive systems, and scheduling practices. For example, the item "Top management does not regularly talk about anti-fraud policies" loaded at 0.842, and "Employees believe that minor misbehavior goes unpunished" loaded at 0.873.

The second factor called Personnel Management explained 24.17% of the variance and captured items such as "Human resource processes do not include background checks of any kind when hiring" (loading = 0.884) and "Employees are not rotated among departments" (loading = 0.856) and "Performance reviews do not assess risk of fraud" (loading = 0.803). These items relate to how the various employment and personnel management practices of an organization may deter or enable fraud.

The third factor, Compliance with Standards, explained 21.03% of the variance and included items that related to documented internal control policies, written guidelines on ethics, and mandatory ethics training. For example, the item "Internal control procedures are seldom audited for compliance" loaded 0.857, and "Ethics training is neither mandatory nor periodic" loaded 0.829.

The fourth factor, Risk Management, explained 12.26% of the variance and included items associated with verbal or documented compliance processes, risk assessment policies, and whistleblower policies. The most informative example was "We have no written policies or procedures for fraud risk management," which loaded at 0.858, and "We have no independent whistleblower hotline," which loaded at 0.815.

The existence of these four factors conveys that the vulnerabilities of institutions to commit fraud are much more complex than shortcomings in procedural controls. They are also inherent vulnerabilities of culture, human resources, and compliance. Leadership and Culture work together and illustrate the degree to which the values of the organization and top management philosophies of an institution are reflected in day-to-day behaviour. Recruitment and Personnel Management outline how the appointment, training, and rotation of employees may hinder or promote instances of fraud. Control and Ethics comprise the formalized policies, training, and monitoring schemes to deter wrongdoing. Finally, Compliance and Risk Management emphasize the value of ascertaining the degree to which institutions have explicit frameworks for risk assessment, whistleblower protections, and explicit rules to comply with that deter offending behaviour.

Figure 2. Factor Components

F1 = .841Q1 +.875Q5 +.862Q12 +.855Q16 +.847Q20 +.871Q28

F2 = .826Q2+ .884Q14 +.842Q17 +.865Q26 + .883Q30

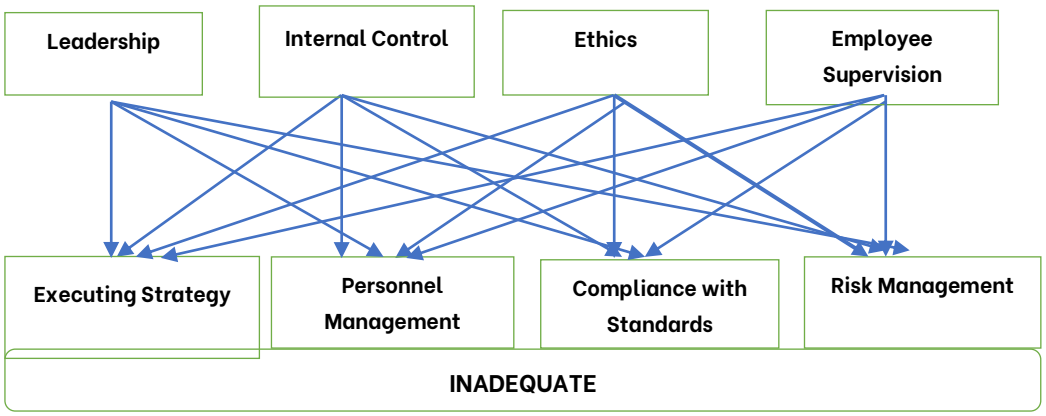
F3 = .857Q3 + .858Q11 + .850Q15 + .829Q18 + .858Q27

F4 = .815Q4 + .858Q13 + .816Q19 + .856Q29

The results of the component transformation matrix show an achievement of an Executing strategy, Personnel Management, Compliance with Standards, and Risk Management, which has substantially contributed to financial fraud within the organization. From these results, it has been characterized four major factors of financial fraud to occur against organizations.

The organizations have four major weaknesses that can provide the context for employee and external financial fraud, according to Figure 3. The findings revealed that the organization had an incomplete execution strategy, which could foster financial fraud. Financial fraud enables organizations to do more with less or at a value for money through more straightforward mergers or streamlined acquisitions - the job descriptions and executions would generally be more effective and alternatively efficacious. It should include strategic planning, communications, goal setting, tracking reports, performance management, and rewards and remuneration.

Figure 3. Details of the Factors



Compliance suggests having regard to certain rules, standards, procedures, norms, or statutes. Regulatory compliance refers to the organization's desired outcome resulting from undertaking steps to identify and ensure that it complies with relevant legislation and regulations. The lack of laws, regulations, and

DOI: 10.5281/zenodo.15564108

policies, or the destruction of existing legal statutes, serves as the most substantive background for financial crime or fraud. It is simply the "non-compliance" with rules or "non-compliance" with "accepted principles."

This research emphasizes that a deficiency of Personal or Human resource management contributes to financial fraud. Human Resource Management is the management of acquiring, using, and maintaining a comfortable workforce. It is a significant contributor to the organization as those who work and are formed in partnership within the organization. It is the major pull factor for their internal employees to engage in this sort of crime. The research emphasizes that a lack of risk management has contributed to financial fraud. Risk management is the process of managing risks to the resources and assets of the company, which can arise from diverse challenges or hazards, including fraud, financial uncertainty, legal liability, strategic failures in management, incidents, or natural disasters, which have led to an increase in substandard risk management in organizations.

6. Discussion

This research utilized the general theoretical frameworks to analyze institutional imperfections that precipitate instances of financial fraud, including the Fraud Triangle (Cressey, 1953) states that opportunity, pressure, and rationalization must all exist simultaneously for fraud to occur. The Fraud Diamond (Wolfe & Hermanson, 2004) added the fourth element of capability, which specifies that fraud is executed by people with the necessary delinquent credentials. Understanding these frameworks will help identify the institutional weaknesses that are the focus of this study.

Based on the theoretical frameworks of the Fraud Triangle and Fraud Diamond the discussion below integrates how deficiencies of leadership, organizational culture, internal controls, ethical climate and compliance intersect to create enablers of crimes, as well as the data trends emphasized the relative importance of social factors—norms, values and rationalizations—that may surpass economic motivations. Each of the core themes is examined in detail, and implications for theory, practice, and policy are stated.

6.1 The Primacy of Leadership and Organizational Culture

The study's quantitative evidence uniformly implicates the responsibility of leadership in an organization's susceptibility to fraud. I showed that, in the regression analysis, the effectiveness of leadership was the most important protective factor, with a beta coefficient of −0.340 ($p < .001$). Simpson (2002) and Rae and Subramaniam (2008) found that when leaders do not demonstrate ethical

behavior and emphasize fraud prevention, lower-level employees may perceive that committing questionable acts is acceptable or implicitly encouraged.

The idea that the behavior of leaders governs the ethical tone of an organization is well established in the corporate governance literature; however, it is particularly salient in contexts such as Sri Lanka when power hierarchies and high power-distance ideologies may preclude subordinates from questioning their leader. Activists and policy advocates must realize that improving organizational fraud prevention is not simply a journey to develop new controls, but developing a sense of ethical leadership that is pervasive through all levels of the organization.

6.2 Internal Controls, Technology, and the "Opportunity" Element

Weak internal controls were shown to be a strong risk factor in both the regression and factor analyses. The negative coefficient for internal control systems ($\beta = -0.317$, $p < .001$) implies that strong internal controls drastically reduce the likelihood of fraud. The PCA indicates that control and ethics were identified as separate constructs that accounted for 21.03% of the variance. These results appear to correlate with the "Opportunity" component of the Fraud Triangle, because if an organization does not ensure rigorous checks and balances are in place in their systems, they provide offenders with an opportunity to commit fraud with little risk.

Under the "opportunity" component, technical deficits are key. Many organizations in Sri Lanka are still using legacy systems or manual systems, or are somewhere in the middle between manual record keeping and tech devices. When an organization is transitioning between legacy systems to real-time systems or is not monitoring a system's audit trail, it provides fraudsters with an environment that allows them to tamper with a record without leaving a trail. Organizations need to think beyond just digitizing, as many organizations are trying to ensure nothing is done on paper; this does not resolve problems. Organizations must establish an internal control system that enables an end-to-end, real-time monitoring system, allowing ICT fraud alerts to be raised, enforcing access restrictions, and ensuring users have adequate training on how to use the system properly. If organizations are not going to put controls in place, they are going to continue to have weak controls while still having the "opportunity" to commit fraud.

6.3 Ethical Climate and Rationalization

The regression analysis revealed that ethical climate is a strong and negative predictor ($\beta = -0.289$, $p < .001$) of fraud frequency. This study demonstrates the significance of a strong ethical culture that involves a code, ethics training, and enforcement to prevent fraud.

DOI: 10.5281/zenodo.15564108

The relationship between moral justification and organizational culture is important to mention. In organizations where unethical actions by senior managers occurred, lower-level employees believed this conveyed a message that such behavior was acceptable. Rationalizations like "everyone is doing it" and "the organization does not care" began to emerge. Such rationalizations echo the rationalization part of Cressey's Fraud Triangle and correspond to the work of Mackevičius and Giriūnas (2013), which supports the notion that when cultures allow minor infractions, these can become greater infractions over time. Addressing this requires acknowledging all minor violations and fostering a culture that explicitly mentions ethical breaches of all kinds, while simultaneously promoting personal accountability for actions taken at the individual level and collective dialogue on ethical issues.

6.4 Recruitment, Personnel Management, and the "Capability" Dimension

Cressey's Fraud Triangle considers pressure, opportunity, and rationalization, but Wolfe and Hermanson's Fraud Diamond adds capability, bringing attention to the individual skill set and position of the offender. In this study, the factor analysis resulted in Recruitment and Personnel Management as a separate individual dimension, with 24.17% of the variance. This study's findings correspond with Gbegi and Adebisi's (2013) focus on the "capacity" dimension, along with Crowe's (2011) notion of propensity, which demonstrates that they are confident in the belief that they can outsmart the current systems.

To mitigate these risks, organizations must enhance recruitment levels that include background checks, competency tests, and reference checks. They should also attempt to continuously rotate employees from function to function, particularly those in financial control roles, limiting the amount of tacit knowledge that the offenders can use. Awareness of fraud risk should be included in performance reviews, enhancing clarity around fraud risk should be acquired by supervisors so they should monitor both the employee's output while examining their adherence to the control procedures. By emphasizing the capability dimension through robust personnel management procedures, organizations can decrease the probability of sophisticated insiders perpetrating fraud.

6.5 Compliance, Risk Management, and Broader Contextual Pressures

The fourth factor determined by PCA – Compliance and Risk Management – emphasizes the need for stronger, formalized policies relating to fraud risk management, comprehensive frameworks for assessing risk, and reporting channels that are accessible and are known to support workers at risk of reprisal.

Interviews indicated that, in some organizations, there were no fraud risk management policies, they were dated, or they were not communicated widely. When there were policies, associated enforcement was random, and reporting channels for whistleblowers were either non-existent or apathetic to workers' complaints. The combination of these facts engendered a sense of "impunity" amongst offenders and further reinforced the "opportunity" aspect within the Fraud Triangle.

Notice that the regression model revealed the political environment to be a significant positive predictor of fraud incidence ($\beta = 0.146$, $p = .011$), which highlights the situational context that pressures institutional responses. Bureaucratic disruption, political favoritism, and public sector agencies' corruption create an environment in which fraud could happen and might be implicitly authorized. Similarly, private firms are not immune to contextual pressures, such as competition and pressure to achieve performance targets. These findings align with Holtfreter's (2005) assertion that performance pressure can become a powerful motivator for organizational crime. Thus, new compliance and risk management cannot merely be about developing policies but changing the culture through the re-ordering of performance-based incentives to achieve sustainable, ethical performance.

7. Conclusion

This study has focused on identifying the structural factors that promote financial fraud in Sri Lanka, using quantitative investigations of data from 435 institutions. It finds that a lack of leadership, weak internal controls, poor ethical climate, ineffective recruitment, and weak compliance procedures combine to create institutional conditions in which fraud can flourish. The data indicate that social factors, such as organizational culture, rationalization, and political interference, are often more important than economic factors, indicating that a systemic approach to fraud is needed as a socio-institutional, rather than simply a technical, issue.

The key quantitative findings show that leadership effectiveness, internal controls, and ethical climate have significant and negative causal links to the incidence of fraud, while organizations with poor ethical climates and problematic political institutional arrangements add to risk. The four factors emerging from factor analysis (Leadership and Culture, Recruitment and Personnel, Control and Ethics, and Compliance and Risk Management) each accounted for a significant part of the variance in vulnerability to fraud.

From a theoretical perspective, the research supports and expands theoretical frameworks such as the Fraud Triangle and Fraud Diamond by demonstrating that each of the theoretical components—pressure, opportunity, rationalization, and

DOI: 10.5281/zenodo.15564108

capability—is manifested differently in the Sri Lankan situation. The evidence of political and cultural aspects also illuminates the need to situate fraud theory within the broader socio-economic situation. These findings suggest important areas of future research that could incorporate macro-level aspects into fraud theory.

From a practical perspective, the research also provided a broad range of recommendations for policymakers, regulators, and organizational leaders. Increasing leadership commitment through visible expressions of ethical programs, improving internal controls and technology processes, developing an ethical culture, more sophisticated recruitment and human resource decisions, better compliance and risk management, and addressing the broader political and regulatory external influences. The author asserts that Sri Lankan organizations will have a substantial reduction in risk of fraud by taking a coordinated approach to integrate the recommendations in this study while preserving the trust of all stakeholders and promoting sustainability.

In conclusion, financial fraud in Sri Lanka is a complex challenge that is multifaceted in nature and will require holistic solutions. By addressing the institutional vulnerabilities highlighted in the study and promoting integrity, Sri Lankan organizations and policymakers can begin to move toward greater resilience. The elements of strong leadership, comprehensive controls, ethical norms, and compliance will serve to provide a deterrent against fraudulent behaviour, while also building the good governance fundamentals required for sustainable economic and social development.

8. Limitations and Directions for Future Research

The study has several limitations that should be mentioned. First, while 435 institutions provide a considerable level of breadth and depth, the findings should not be fully generalized to organizations in other districts or to sectors that work under entirely different regulatory regimes. Second, the data are cross-sectional, making it difficult to draw inferences about causation. Longitudinal studies would help to track institutional changes and how these changes, together with social conditions, influence fraud rates over time. Third, data collected through self-reported questionnaires may suffer from response bias, although the high reliability coefficients and the triangulation with qualitative narratives mitigate some concern.

Future research should extend the work further by examining the effectiveness of different interventions, such as ethics training programs or technology upgrades, on fraud rate reductions. Additionally, research that compares organizations in the

South Asian region may be especially valuable for discerning patterns and best practices so that these can be more broadly shared across different contexts. Furthermore, as financial crime includes cyber-fraud and increasingly varied emerging threats, expanding to this issue would help to ensure that academic research keeps up with the changing landscape of financial crime.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding Information

No funding was received for this research. The study was conducted independently, with institutional support from the University of Sri Jayewardenepura.

Ethical and Originality Statement

The Author declares that this work is original and has never been published in any form or any other media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.

References

Adeduro, A. A. (1998). An investigation into frauds in banks (Unpublished master's thesis). University of Lagos.

Albrecht, W. S., Albrecht, C. C., & Albrecht, C. O. (2006). *Fraud Examination* (2nd ed.). Mason, OH: Thomson Southwestern.

Alleyne, P., & Howard, M. (2005). An exploratory study of auditors' responsibility for fraud detection in Barbados. *Managerial Auditing Journal*, *20*(3), 284–303.

Apostolou, B., & Apostolou, N. (2013). The value of risk assessment: Evidence from a recent survey of forensic examiners. *Forensic Examiner*, *21*(3), 14–22.

Bressler, L., & Bressler, M. (2007). A model for prevention and detection of criminal activity impacting small businesses. *Entrepreneur Executive*, *12*, 23–36.

Bussmann, D., & Werle, M. (2005). Addressing crime in companies. *British Journal of Criminology, 46*(6), 257–299.

Cressey, D. R. (1953). *Other People's Money: A Study in the Social Psychology of Embezzlement*. Glencoe, IL: Free Press.

Crowe, W. A. (2011). Introducing the Fraud Pentagon: Adding two elements to the fraud triangle. *Journal of Corporate Accounting & Finance, 22*(5), 57–60.

DOI: 10.5281/zenodo.15564108

Gbegi, D. O., & Adebisi, J. F. (2013). The new fraud diamond model: How can it help forensic accountants in fraud investigation in Nigeria? *European Journal of Accounting Auditing and Finance Research, 1*(4), 129–138.

Golden, T. W., Skalak, S. S., & Clayton, M. M. (2006). *A Guide to Forensic Accounting Investigation*. Hoboken, NJ: John Wiley & Sons.

Gottschalk, P. (2010). Theories of financial crime. *Journal of Financial Crime, 17*(2), 210–222. https://doi.org/10.1108/13590791011033908

Gunawardene, K. D. (2015). An empirical investigation of computerized accounting information systems fraud in licensed banks in Sri Lanka. In *Proceedings of the 1st International Conference in Accounting Researchers and Educators* (pp. 1–21). University of Kelaniya.

Holtfreter, K. (2005). In occupational fraud, "typical" white-collar crime? A comparison of individual and organizational characteristics. *Journal of Financial Crime, 17*(2), 295–307.

Jayasinghe, D., & Ajward, R. (2019). The level of usage and importance of fraud detection and prevention techniques in Sri Lankan banking institutions: Perceptions of internal and external auditors. *CA Journal of Applied Research, 3*, 158–180.

Kenyon, W., & Tilton, P. D. (2006). Potential red flags and fraud detection techniques: A guide to forensic accounting investigation (1st ed.). Hoboken, NJ: John Wiley & Sons.

Mackevičius, J., & Giriūnas, L. (2013). Transformational research of the Fraud Triangle. *Ekonomika, 92*(4), 1–15.

Mangala, D., & Pooja, K. (2015). Corporate fraud prevention and detection: Revisiting the literature. *Journal of Commerce and Accounting Research, 4*(1), 1–12.

Marsoof, S. (2003). Taking the profit out of crime—Sri Lankan style. *Journal of Financial Crime, 10*(4), 350–364.

McGurrin, D. (2013). The theft of a nation symposium: Introduction. *Western Criminology Review, 14*(2), 20–22.

Rae, K., & Subramaniam, N. (2008). Quality of internal control procedures: Antecedents and moderating effect on organizational justice and employee fraud. *Managerial Auditing Journal, 23*(2), 104–124.

Redford, A. (1928). Economic history of Europe to the end of the Middle Ages. *Journal of Accountancy, 177*(1), 60–66.

Simpson, S. S. (2002). *Corporate Crime, Law, and Social Control*. Cambridge, UK: Cambridge University Press.

Samarasinghe, D. S., Muthuswamy, G., & Jayaweera, K. (2018). Auditors' constraints in detecting and reporting client illegal acts: Evidence from Sri Lanka. *International Journal of Accounting and Auditing, 15*(1), 29–45.

Sujeewa, G. M. M., Kaushalaya, M. D. P., & Manawaduge, A. (2018). Using Beneish M-Score model to detect red flags of corporate financial statement fraud in Sri Lanka. *The Journal of Applied Research, 2*, 45–60.

Walsh, J. P., & Seward, J. K. (1990). On the efficiency of internal and external corporate control mechanisms. *Academy of Management Review, 15*(3), 421–458.

Wolfe, D., & Hermanson, D. R. (2004). The Fraud Diamond: Considering four elements of fraud. *The CPA Journal, 74*(12), 38–42.