

Forensic Accounting and Financial Fraud Control in Malaysian SMEs: A Conceptual Framework for Detection, Prevention and Governance

Asreawaney Bt Mod Ishak*

Faculty of Business, UNITAR International University, 47301 Petaling Jaya, Selangor, Malaysia

*Corresponding Author

DOI: <https://doi.org/10.47772/IJRISS.2026.100800970>

Received: 07 September 2026; Accepted: 12 September 2026; Published: 22 September 2026

ABSTRACT

Financial fraud can be disproportionately damaging to small and medium enterprises (SMEs) because a loss that a large organisation can absorb may disrupt the liquidity, reputation and continuity of a smaller firm. This conceptual paper develops a Malaysia-focused framework explaining how forensic accounting is expected to support financial fraud-control effectiveness under SME resource constraints. An integrative conceptual review was undertaken, drawing primarily on peer-reviewed research published from 2018 to 2026, supplemented by foundational theory and authoritative institutional guidance. The synthesis treats forensic accounting as an organisational capability comprising access to investigative accounting expertise, fraud-risk diagnosis, evidence evaluation and disciplined inquiry rather than as a post-event service alone. The proposed mechanism is sequential. Forensic accounting capability is expected to improve fraud detection and diagnostic insight; those insights are expected to support preventive control remediation; and effective remediation is expected to contribute to stronger fraud-control outcomes, including lower exposure, recurrence and loss severity and more timely organisational response. Two boundary conditions are incorporated. Digital and analytical enablement is expected to strengthen the translation of forensic capability into detection and diagnostic insight, while governance, internal controls and an ethical climate that supports challenge are expected to strengthen the translation of diagnostic insight into preventive remediation. White-Collar Crime Theory is used as a sensitising lens for understanding how legitimate occupational access and process knowledge can facilitate concealment, while the causal mechanism is developed from the integrated forensic-accounting and fraud-control literature. Five propositions are advanced for future empirical testing. The framework contributes by separating detection, remediation and fraud-control effectiveness, clarifying where technology and governance enter the process, and offering a proportionate model that Malaysian SMEs can implement through internal, outsourced or hybrid forensic capability.

Keywords: forensic accounting, financial fraud-control effectiveness, Malaysian SMEs, fraud detection, corporate governance

INTRODUCTION

Micro, small and medium enterprises (MSMEs) are central to Malaysia's economic activity. The Department of Statistics Malaysia reported that MSMEs generated RM689.8 billion in value added and accounted for 39.7% of national gross domestic product in 2025 (Department of Statistics Malaysia [DOSM], 2026). Their importance means that weaknesses in financial integrity are not confined to individual owner-managers. Fraud-related losses can affect employees, suppliers, lenders and local business networks, particularly when a smaller firm has limited financial slack.

The exposure of smaller organisations is also structurally different from that of large corporations. SMEs commonly operate with compact finance teams, concentrated authority and relationship-based routines. These features may support flexibility and fast decisions, but they can also weaken segregation of duties, independent review and the visibility of override. The Association of Certified Fraud Examiners (ACFE, 2024) reports that

several occupational fraud schemes, including billing fraud, check and payment tampering, skimming, cash larceny, payroll fraud and financial statement fraud, occur more frequently in small organisations than in larger ones. Malaysian evidence similarly indicates that SMEs face a broad range of fraud schemes while many make limited use of anti-fraud measures (Sow et al., 2018b).

Forensic accounting is relevant because it introduces a form of inquiry that goes beyond routine transaction processing and conventional control checking. It combines financial analysis with investigative and evidential reasoning, drawing on accounting, auditing, digital inquiry and an understanding of legal processes. The focus is not simply whether a record balances, but whether a transaction is commercially plausible, adequately supported and consistent with other financial and operational evidence. Reviews of the field associate forensic accounting with both fraud detection and fraud prevention, while also emphasising the importance of specialist skills, professional judgement and the complexity of fraud investigations (Alshurafat et al., 2021; Guellim et al., 2024; Kaur et al., 2022).

An important conceptual issue remains, however. Much of the literature discusses the benefits of forensic accounting without clearly separating the stages through which those benefits arise. Detecting an unusual transaction is not the same as understanding the control weakness that enabled it, and neither guarantees that the weakness will be corrected. Likewise, analytical software can generate exceptions without management investigating them, while an investigation may identify misconduct without changing the process that allowed the misconduct to recur. The 2023 Fraud Risk Management Guide is useful in this respect because it places preventive and detective controls, investigation, corrective action and ongoing monitoring within one fraud-risk management programme (Committee of Sponsoring Organizations of the Treadway Commission [COSO] & ACFE, 2023).

This distinction matters particularly for SMEs. Most smaller firms cannot reproduce the dedicated forensic departments, specialist teams or technology infrastructure of large corporations. In Malaysia, this resource constraint is especially relevant because MSMEs represent a substantial share of national economic activity while operating across highly varied levels of size, formalisation, governance capacity and digital maturity. Malaysian studies also indicate continued exposure to multiple fraud schemes, limited preventive action in some firms, and the importance of internal control, fraud awareness, honesty, integrity and oversight (Sow et al., 2018a, 2018b; Bakar et al., 2023). A useful conceptual model must therefore explain not only whether forensic accounting matters, but how its value is generated and under what conditions that value can be realised with proportionate resources. Recent reviews identify technology, governance, specialist capability and institutional development as recurring themes in forensic-accounting research (Airout et al., 2024; Ozili, 2023; Singh & Kumari, 2025). Recent SME-focused conceptual work also treats forensic accounting expertise as an organisational resource that can support threat detection and the reconfiguration of controls in resource-constrained settings (Awolowo et al., 2026).

Accordingly, this paper develops a conceptual framework for financial fraud control in Malaysian SMEs. It has three objectives. First, it conceptualises forensic accounting as an organisational capability that can be accessed internally, externally or through a hybrid arrangement. Second, it distinguishes fraud detection and diagnostic insight from preventive control remediation and from the eventual effectiveness of fraud control. Third, it identifies two boundary conditions: digital and analytical enablement at the detection stage, and governance, internal controls and ethical climate at the remediation stage.

The paper contributes by making the causal sequence more explicit. Rather than assuming a direct and uniform relationship between forensic accounting and lower fraud, the framework proposes that forensic capability first improves the quality of detection and diagnosis; diagnostic insight then supports targeted remediation; and remediation strengthens financial fraud-control effectiveness. White-Collar Crime Theory is used as a sensitising lens for the problem of legitimate occupational access and concealment, while the organisational mechanism is developed from the integrated literature on forensic accounting, fraud-risk management and SME controls. This produces five propositions that can be tested empirically in Malaysia and other comparable SME settings.

LITERATURE REVIEW AND CONCEPTUAL BACKGROUND

Forensic accounting as an organisational capability

Forensic accounting combines financial analysis with investigative and evidential reasoning, drawing on accounting, auditing, digital inquiry and an understanding of legal processes. Its distinctive feature is therefore not a single test but an orientation toward questioning, corroboration and reconstruction. Tiwari and Debnath (2017) describe the field as a blend of knowledge extending beyond routine accounting competence, while Howieson (2018) highlights the judgement and ethical qualities expected of the forensic practitioner. Alshurafat et al. (2021) similarly show that the profession's value is linked to specialised expertise but is constrained by uneven professional development and shortages of highly qualified practitioners.

A capability perspective is useful for SMEs because it separates the value of forensic expertise from the employment model through which that expertise is obtained. In this paper, forensic accounting capability refers to an SME's ability to access and deploy investigative accounting expertise when financial anomalies, allegations or high-risk processes require deeper examination. It can be internal, outsourced or hybrid. Core elements include fraud-risk diagnosis, transaction tracing, document examination, interview and inquiry skills, evidence preservation, analytical review and the ability to communicate findings in a form that supports managerial or legal action.

This framing is consistent with wider reviews. Kaur et al. (2022) identify both fraud detection and prevention as central contributions of forensic accounting, while Guellim et al. (2024) show that perceived value spans services, professional skills, standards and education. Awolowo et al. (2026), writing specifically about SMEs, conceptualise forensic accounting expertise as a knowledge resource that can enhance the ability to sense threats and reconfigure organisational responses. These studies support a capability-based view without implying that every SME requires a permanent forensic specialist.

Fraud vulnerability in SMEs

SMEs are not inherently less ethical or less competently managed than larger organisations. Their vulnerability follows from structural trade-offs. A compact finance function may allow close owner oversight and faster decisions, but the same person may initiate, authorise, record and reconcile transactions. Long-standing relationships may support trust and flexibility while reducing the perceived need for independent verification. Informal routines can lower administrative cost but leave a weak evidence trail when a dispute or suspected fraud occurs.

Malaysian research illustrates this problem. Sow et al. (2018b) found that SMEs were exposed to a broad range of fraud schemes even though relatively few had taken preventive action. Nawawi and Salin (2018), in a Malaysian occupational-fraud case, identified weaknesses in expenditure-claim controls and showed how the work environment and control design can affect fraud risk. Bakar et al. (2023) subsequently found that internal control and fraud awareness significantly influenced the tendency toward occupational fraud among Malaysian SME employees. Hashim et al. (2020), although not confined to SMEs, also demonstrate that financial-fraud risk is shaped by managerial and organisational conditions.

The consequences can be especially disruptive for smaller firms. Cash losses may affect payroll or supplier payments, manipulation of financial records can affect access to credit, and reputational damage can be difficult to repair in relationship-based markets. The preventive value of an investigation therefore remains limited if the control weakness that enabled the misconduct is not corrected after the case is resolved. This makes the movement from detection to diagnosis and then to remediation central to the framework developed here.

From detection and diagnosis to preventive remediation

Detection, diagnosis and prevention perform different but complementary functions. Detection concerns identifying indicators that misconduct may have occurred or may be occurring. Diagnostic insight concerns understanding what the anomaly means, how the transaction or scheme operated, which control was bypassed

and what evidence supports the conclusion. Preventive control remediation occurs when that learning is translated into changes to responsibilities, authorisations, access, monitoring or other controls so that the same weakness is less likely to be exploited again.

Forensic accounting contributes to the first two stages by focusing attention on patterns that routine processing may overlook and by testing explanations against evidence. Depending on the risk, this can involve unusual vendor relationships, duplicate or split payments, transactions close to approval thresholds, inconsistent supporting documents, unexplained manual journals, abnormal margins or mismatches between financial and operational records. An anomaly is not treated as proof of fraud; it is a reason for proportionate inquiry.

The prevention literature becomes more useful when it is read through this diagnostic-remediation sequence. Kaur et al. (2022) conclude that forensic accounting contributes to both detection and prevention. Hasan et al. (2024) connect forensic accounting with internal audit systems and governance, while Oladejo and Olorunsola (2023) report a positive relationship between forensic-accounting practices and fraud prevention in owner-managed SMEs. Importantly, COSO and ACFE (2023) place investigation and corrective action alongside preventive and detective controls and state that discovered fraud should be thoroughly remediated. The implication is that investigative knowledge creates preventive value when the organisation changes the process that generated the risk.

Governance, internal controls and ethical climate

Forensic insight does not automatically produce control improvement. An exception report may identify a suspicious transaction, but someone must have the authority and willingness to investigate it. A recommendation to separate incompatible duties may be technically sound, but an owner-manager may resist the additional cost or inconvenience. Governance, internal controls and ethical climate therefore shape whether diagnostic insight is converted into preventive remediation.

Malaysian evidence supports this emphasis. Sow et al. (2018a) found that a culture of honesty and integrity, anti-fraud processes and controls, and appropriate oversight were positively associated with fraud prevention in Malaysian SMEs. Bakar et al. (2023) also found that internal control and fraud awareness were significant in explaining occupational-fraud tendency. Related Malaysian research also emphasises the role of internal-control components in safeguarding funds and strengthening accountability in resource-constrained private institutions (Ibrahim et al., 2023). At a broader organisational level, Murphy and Free (2016) show that an instrumental climate - one in which self-interest or organisational interest displaces ethical concerns - is associated with fraud-related pressures and rationalisations. These findings suggest that formal controls and the social response to challenge need to be considered together.

The present framework therefore treats governance, internal controls and ethical climate as conceptually distinct but complementary conditions at the remediation stage. Governance concerns oversight, authority and accountability for acting on difficult findings; internal controls concern the formal procedures, access restrictions, approvals and monitoring mechanisms through which identified weaknesses are corrected; and ethical climate concerns whether challenge, escalation and reporting are supported rather than discouraged. They are grouped as a second-stage boundary condition because each affects whether diagnostic insight is translated into implemented preventive remediation, not because they are assumed to be interchangeable constructs. The point is not that SMEs need the governance architecture of listed companies. Proportionate mechanisms can include dual approval for high-risk payments, independent bank reconciliation, periodic external review, restricted access, documented related-party transactions and a route for raising concerns outside the immediate reporting line. COSO and ACFE (2023) similarly emphasise fraud-risk governance, investigations, corrective action and monitoring while specifically recognising the circumstances of smaller entities.

Digital and analytical enablement

Digital records have expanded the practical reach of forensic work. Transactions can now be screened for unusual relationships, duplicates, timing patterns, access anomalies and other exceptions that would be

difficult to identify through manual review alone. Bibliometric and systematic reviews increasingly place data analytics, artificial intelligence and related technologies within the forensic-accounting research agenda (Airout et al., 2024; Singh & Kumari, 2025). Isa and Tazilah's (2026) scoping review of 116 empirical studies likewise identifies technology-based fraud detection as a dominant theme, while continuing to identify auditor or professional oversight, governance and internal controls as important complements to technology. Malaysian evidence from insurance-fraud classification further demonstrates that machine-learning models can assist in identifying potentially fraudulent claims, illustrating the detection value of data-driven analytical methods (Nordin et al., 2024).

For SMEs, digital enablement should be interpreted pragmatically rather than as a requirement to purchase sophisticated artificial-intelligence systems. Duplicate-payment tests, exception reports, vendor matching, access-log review and targeted trend analysis can materially increase the coverage of inquiry when they are matched to the firm's transaction profile. COSO and ACFE (2023) explicitly incorporate data analytics into fraud preventive and detective control activities, and recent SME-focused work argues that forensic expertise should be integrated with wider organisational capabilities rather than treated as a technology substitute (Awolowo et al., 2026).

Analytical technologies can identify unusual patterns, but the interpretation of those patterns still requires professional assessment of context and evidence. Poor-quality data can produce weak signals, automated models may flag legitimate transactions, and small firms may lack staff able to validate outputs. For this reason, digital and analytical enablement is positioned in the framework as a condition that strengthens the first-stage relationship between forensic accounting capability and detection and diagnostic insight, not as an internal dimension that duplicates forensic capability itself.

Financial fraud-control effectiveness

To avoid treating detection and prevention as both causes and outcomes of the same construct, the framework distinguishes financial fraud-control effectiveness from the mechanisms that precede it. Financial fraud-control effectiveness refers to the extent to which an SME reduces its exposure to financial misconduct, limits recurrence and loss severity, responds to suspected fraud in a timely manner and maintains credible accountability after an incident. It is therefore an outcome of the fraud-control process rather than another label for detection or prevention.

This distinction is consistent with the logic of contemporary fraud-risk management. ACFE (2024) documents the material consequences of occupational fraud, while COSO and ACFE (2023) present prevention, detection, investigation, corrective action and monitoring as connected elements of a broader programme. The conceptual question is thus whether an SME can convert forensic capability and investigative learning into a demonstrably stronger control environment over time.

Theoretical Lens

White-Collar Crime Theory

White-Collar Crime Theory is used here as a sensitising theoretical lens rather than as a complete causal model for every relationship in the framework. Sutherland (1949) challenged the assumption that serious offending was confined to socially marginal groups and directed attention to offences committed by respectable individuals in the course of occupation. For financial fraud, the important implication is legitimate access. People who understand an organisation's systems, routines, documentation and authority structure may be unusually well placed to conceal misconduct within activities that appear ordinary.

This perspective is particularly relevant to SMEs because access and responsibility are often concentrated. A manager, family member or long-serving employee may control several stages of a transaction and may also possess contextual knowledge that helps explain away an irregularity. Trust can lower coordination costs and support efficient operations, yet it can delay challenge when an individual with legitimate authority deviates from expected behaviour. The theory therefore draws attention to the concealment advantage that can arise from occupational position and process knowledge.

Implications for the conceptual mechanism

The theoretical lens informs why forensic accounting capability is necessary at the first stage of the framework. White-Collar Crime Theory draws attention to misconduct committed through legitimate occupational roles and therefore to the informational advantage available to insiders who understand transaction flows, documentation routines and control weaknesses. In the present framework, forensic inquiry responds to that concealment advantage by introducing corroboration, traceability and independent challenge. It asks whether the recorded transaction is supported by evidence from other sources, whether the explanation is consistent with commercial reality and whether the control environment made manipulation unusually easy. The theory is therefore used to explain the access-and-concealment problem that motivates forensic detection and diagnosis, while it is not extended beyond its explanatory scope to account for technology adoption or the organisational implementation of remediation.

The organisational sequence proposed in this paper is then developed from the integrative fraud-control literature. Detection makes questionable activity visible; diagnostic inquiry identifies how the activity was enabled; preventive remediation changes the relevant control; and stronger controls contribute to fraud-control effectiveness. Digital and analytical enablement affects how much financial activity can be screened and interrogated, while governance and ethical climate influence whether difficult findings are acted upon. White-Collar Crime Theory therefore sensitises the analysis to access and concealment, whereas the forensic-accounting and fraud-risk literature supplies the operational mechanism.

METHODOLOGY

Review design

This study uses an integrative conceptual review. Integrative reviews are appropriate when a research problem spans several literatures and the objective is to synthesise concepts in a way that produces a new framework rather than to estimate a pooled effect size (Snyder, 2019; Torraco, 2016). The present question requires evidence from forensic accounting, SME fraud, internal control, governance, ethical climate and digital analytics. A narrowly defined systematic review of only one of those domains would not by itself answer how the elements fit together.

The review is therefore designed for conceptual integration rather than exhaustive evidence counting. Peer-reviewed journal articles form the main evidence base, supplemented by authoritative institutional publications for current fraud-risk guidance and Malaysian economic context. Older work is retained where it provides the theoretical foundation, while recent literature is emphasised where technology and practice are changing quickly.

Source identification and selection

Sources were identified through targeted keyword searches of web-accessible scholarly indexes and publisher platforms, supplemented by backward reference chaining from established review articles. Because the study was designed as an integrative conceptual review rather than a systematic review, source identification was not restricted to a predefined closed set of databases and no claim of exhaustive database coverage is made. Search combinations included 'forensic accounting', 'fraud detection', 'fraud prevention', 'fraud control', 'SME', 'small business', 'internal control', 'ethical climate', 'corporate governance', 'data analytics', 'digital forensics' and 'Malaysia'. The principal publication window was 2018-2026, although earlier sources were retained when they established a core theoretical, methodological or professional concept. This approach is reported transparently to distinguish the review from a protocol-driven systematic review and to avoid implying reproducibility beyond the integrative purpose of the study.

A source was retained when it directly informed at least one construct or relationship in the emerging framework and its bibliographic details could be traced to a publisher, DOI record or authoritative institutional source. Sources were excluded when the connection to financial fraud or accounting was remote, when publication details could not be reliably verified, or when the cited study did not support the claim for which it

was being considered. The literature base was iteratively expanded whenever a proposed construct or relationship rested too heavily on a single source.

The final synthesis reported in this manuscript draws on 26 cited sources: 22 peer-reviewed journal articles, three authoritative institutional publications and one foundational monograph. This count is reported to make the evidential base transparent; it is not presented as an exhaustive population of the forensic-accounting literature. Consistent with the integrative purpose, no PRISMA flow diagram or claim of systematic exhaustiveness is made.

Analytical approach

The selected literature was read comparatively around five questions: (1) what capability distinguishes forensic accounting from routine accounting activity; (2) what makes SMEs vulnerable to financial fraud; (3) how forensic capability improves detection and diagnosis; (4) how diagnostic insight is converted into preventive control change; and (5) what organisational and technological conditions affect those relationships. The first coding stage grouped findings descriptively; the second stage examined the connections and boundary conditions across those groups.

This iterative synthesis produced a serial mechanism rather than two parallel outcomes. Forensic accounting capability supports fraud detection and diagnostic insight; diagnostic insight informs preventive control remediation; and effective remediation strengthens financial fraud-control effectiveness. Digital and analytical enablement is positioned as a first-stage amplifier, while governance, internal controls and ethical climate are positioned as a second-stage boundary condition. The revised structure avoids treating technology simultaneously as a component and moderator of forensic capability and avoids defining fraud control through the same dimensions used to predict it.

Literature Synthesis And Conceptual Framework

Table 1: Representative evidence informing the revised conceptual framework

Source	Evidence / context	Contribution to framework
N'Guilla Sow et al. (2018b)	Survey of 126 Malaysian SMEs; firms faced a broad range of fraud schemes while preventive action was limited.	Anchors SME fraud vulnerability and the need for observable, risk-based controls in Malaysia.
N'Guilla Sow et al. (2018a)	Malaysian SME evidence showing positive roles for honesty and integrity, anti-fraud processes and appropriate oversight in fraud prevention.	Supports governance, internal controls and ethical climate as conditions for remediation.
Bakar et al. (2023)	Malaysian SME survey; internal control and fraud awareness significantly influenced occupational-fraud tendency.	Strengthens the Malaysian evidence for second-stage organisational conditions.
Kaur et al. (2022)	Systematic review of forensic accounting and fraud detection/prevention.	Supports the capability-to-detection relationship and the distinction between detection and prevention.
COSO & ACFE (2023)	Professional guidance integrating governance, assessment, preventive/detective controls, investigation, corrective action and monitoring, with smaller-entity and data-analytics considerations.	Supports the serial logic from detection/investigation to corrective remediation and broader fraud-control effectiveness.

Guellim et al. (2024)	Systematic review of perceived forensic-accounting value across services, skills, standards and education.	Supports a capability-based rather than single-technique definition of forensic accounting.
Murphy & Free (2016)	Empirical evidence that an instrumental organisational climate is associated with fraud-related pressures and rationalisations.	Supports ethical climate as part of the boundary condition affecting organisational response.
Isa & Tazilah (2026)	Scoping review of 116 empirical studies; technology-based detection is prominent while professional oversight, governance and internal controls remain relevant.	Supports digital/analytical enablement as an amplifier rather than a substitute for judgement and control.
Awolowo et al. (2026)	SME conceptual framework treating forensic accounting expertise as a strategic knowledge resource within a resource-constrained setting.	Supports SME-level capability framing and the idea that investigative knowledge can contribute to reconfiguring organisational responses.

Forensic accounting capability and fraud detection and diagnostic insight

The first proposed relationship concerns visibility and understanding. Fraud persists when manipulated activity cannot be distinguished from legitimate transactions or when an anomaly is noticed but not adequately explained. Forensic accounting capability improves this stage by combining accounting knowledge with inquiry: the practitioner examines the amount recorded, the commercial explanation, the supporting documents, the parties involved and the pattern across time.

This approach is particularly useful in SMEs because routine review may rely heavily on familiarity with employees and suppliers. Forensic inquiry introduces corroboration rather than automatic acceptance. Analytical procedures can identify an exception, but document review, transaction tracing and inquiry determine whether the exception has a reasonable explanation or requires deeper investigation. The systematic literature broadly supports the contribution of forensic accounting to fraud detection (Kaur et al., 2022; Guellim et al., 2024).

Proposition 1 (P1): Stronger forensic accounting capability is positively associated with stronger fraud detection and diagnostic insight in Malaysian SMEs.

Fraud detection and diagnostic insight and preventive control remediation

Detection becomes preventive only when the organisation understands why an irregularity occurred and changes the enabling condition. An investigation may show that one employee could create a vendor and approve its payment, that system access was not revoked after role changes, that management review was superficial or that supporting documentation could be generated by the same person who authorised the transaction. Diagnostic insight directs attention to the specific weakness rather than to a generic catalogue of controls.

The resulting remediation can involve separating incompatible duties, changing access rights, requiring independent verification of new vendors, introducing exception reports, improving documentation requirements or redesigning escalation. This logic is consistent with evidence linking forensic work to control improvement and fraud prevention (Hasan et al., 2024; Oladejo & Olorunsola, 2023) and with professional guidance that places investigation and corrective action within the same fraud-risk management cycle (COSO & ACFE, 2023).

Proposition 2 (P2): Stronger fraud detection and diagnostic insight is positively associated with more effective preventive control remediation in Malaysian SMEs.

Preventive control remediation and financial fraud-control effectiveness

The third relationship separates the act of changing a control from the effectiveness of the broader fraud-control environment. A remedial action can be introduced but remain poorly implemented, easily overridden or disconnected from actual risk. Effective remediation is therefore understood as a targeted, implemented and monitored change to the process that enabled or failed to reveal misconduct.

When such changes are sustained, the expected outcome is stronger financial fraud-control effectiveness: lower exposure to repeat schemes, reduced recurrence and loss severity, earlier organisational response and clearer accountability. This outcome is consistent with the programme logic in COSO and ACFE (2023), which connects preventive and detective controls with investigation, remediation and monitoring, and with the practical concern documented by ACFE (2024) that the consequences of occupational fraud can be substantial for smaller organisations.

Proposition 3 (P3): More effective preventive control remediation is positively associated with greater financial fraud-control effectiveness in Malaysian SMEs.

Digital and analytical enablement as a first-stage boundary condition

The value of forensic accounting capability at the detection stage depends partly on what information can be accessed and interrogated. Digital records and analytical tools can increase coverage, identify relationships across transaction populations and direct professional attention toward unusual activity. Recent reviews show growing integration of forensic accounting with data analytics, artificial intelligence and digital-forensic methods (Airout et al., 2024; Isa & Tazilah, 2026; Singh & Kumari, 2025).

The proposed effect is therefore not a direct claim that technology prevents fraud. Rather, digital and analytical enablement should make forensic capability more productive at the point where anomalies are identified and investigated. The same professional expertise can examine more transactions, compare more data fields and identify exceptions earlier when relevant data are available in usable form. In keeping with recent SME capability work, technology is treated as an enabler of organisational inquiry rather than a substitute for professional interpretation (Awolowo et al., 2026).

Proposition 4 (P4): Digital and analytical enablement strengthens the positive relationship between forensic accounting capability and fraud detection and diagnostic insight.

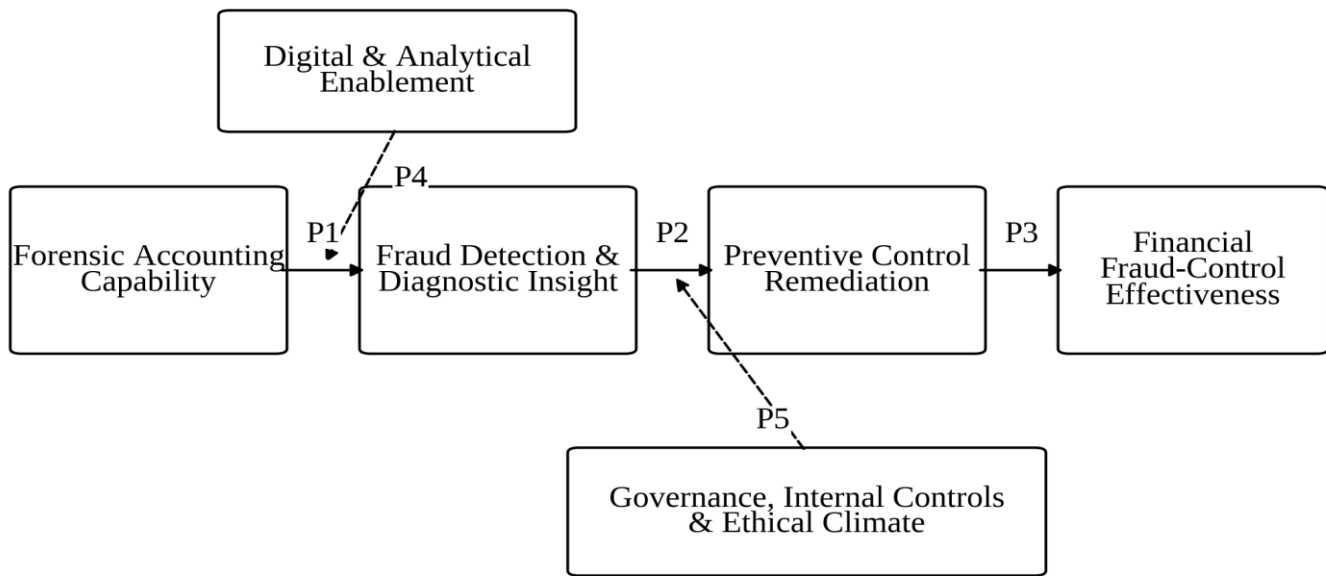
Governance, internal controls and ethical climate as a second-stage boundary condition

The translation of diagnostic insight into preventive change is inherently organisational. A clear finding may still be ignored when the implicated person is powerful, when management regards tighter controls as inconvenient, or when employees believe that raising concerns will be punished. Conversely, an organisation with appropriate oversight and a climate that supports challenge is more likely to use investigation findings to redesign weak processes.

Malaysian SME evidence on honesty and integrity, anti-fraud controls and oversight (Sow et al., 2018a), together with evidence on internal control and fraud awareness (Bakar et al., 2023), supports this boundary condition. Murphy and Free (2016) further demonstrate why the social climate cannot be separated from formal control: a climate that privileges instrumental interests over ethical concerns can contribute to fraud-related rationalisation. Governance, internal controls and ethical climate are therefore expected to determine how reliably diagnostic learning becomes actual remediation.

Proposition 5 (P5): Effective governance, internal controls and an ethical climate that supports challenge strengthen the positive relationship between fraud detection and diagnostic insight and preventive control remediation.

Figure 1: Proposed conceptual framework for forensic accounting and financial fraud control in Malaysian SMEs



Note: Solid arrows represent the proposed direct relationships P1-P3. Dashed arrows represent boundary conditions: digital and analytical enablement strengthens P1, while governance, internal controls and ethical climate strengthen P2. Financial fraud-control effectiveness is defined as an outcome distinct from the preceding detection and remediation mechanisms.

DISCUSSION

The central argument of this paper is that forensic accounting creates value for SMEs through a sequence rather than through a single direct effect. The organisation first needs the capability to interrogate suspicious activity. It then needs sufficient diagnostic insight to understand the enabling weakness. That insight must be converted into a specific preventive change, and the change must be implemented and monitored before it can reasonably be expected to improve fraud-control outcomes. This serial logic helps reconcile research that emphasises specialist investigation with research that emphasises governance and prevention.

The framework also clarifies the place of technology. Analytical technologies can identify unusual patterns, but the interpretation of those patterns still requires professional assessment of context and evidence. A duplicate payment can reflect fraud, error or a legitimate correction; an unusual vendor relationship can be suspicious or commercially necessary. Digital enablement therefore matters most when it increases the reach of a capable investigator rather than when it merely generates more alerts. The technology-focused evidence reviewed by Isa and Tazilah (2026) and Singh and Kumari (2025) supports this interpretation, while Awolowo et al. (2026) similarly position forensic expertise within a broader SME capability system.

A related implication concerns governance. The revised framework does not assume that governance directly creates diagnostic insight. Instead, governance and ethical climate determine whether difficult findings are acted upon. This is important in closely held firms where authority may be concentrated and where commercial relationships can make independent challenge uncomfortable. The empirical Malaysian evidence that anti-fraud controls, oversight and fraud awareness matter (Bakar et al., 2023; Sow et al., 2018a) strengthens the case for placing governance at the remediation stage.

The Malaysian context also reinforces the need for proportionality. MSMEs account for almost two-fifths of national GDP (DOSM, 2026), yet the category covers businesses with very different transaction volumes, systems and managerial resources. Existing Malaysian evidence also points to exposure to diverse fraud

schemes, uneven preventive action, and the importance of internal control, fraud awareness, honesty, integrity and oversight (Sow et al., 2018a, 2018b; Bakar et al., 2023). These conditions make a resource-sensitive framework particularly relevant: the issue is not whether every SME should maintain a specialised forensic unit, but how access to investigative capability can be matched to risk, governance capacity and digital maturity. A microenterprise may obtain meaningful improvement through independent bank reconciliation, access restrictions and periodic external review, whereas a medium-sized manufacturer may justify continuous exception testing, vendor analytics and a more formal fraud-risk assessment. The framework is intended to preserve the same causal logic across those levels without prescribing identical controls.

For SMEs, the objective is not to replace relationship-based trust with excessive control, but to ensure that trust operates within processes that provide appropriate verification and accountability. This distinction is important because small firms often depend on speed and close working relationships. A risk-based approach directs scrutiny toward positions and transactions where access and potential loss are concentrated, rather than subjecting every routine activity to the same level of control.

Theoretical Contributions

The paper makes three theoretical contributions. First, it sharpens the use of White-Collar Crime Theory in the SME fraud context by linking legitimate occupational access to an informational and concealment advantage. This provides a theoretical reason for the framework's emphasis on corroboration, traceability and independent challenge: forensic accounting capability is valuable because it can reduce the informational asymmetry created when trusted insiders understand both organisational processes and the ways those processes can be manipulated. The theory is not extended to explain technology adoption or control remediation; instead, it is used within its appropriate scope to explain why trusted, knowledgeable insiders can be difficult to scrutinise and why detection requires more than routine accounting review.

Second, the framework separates three stages that are often collapsed into a broad claim that forensic accounting 'detects and prevents fraud'. Fraud detection and diagnostic insight is treated as the immediate informational outcome of forensic capability; preventive control remediation is the organisational response to that insight; and financial fraud-control effectiveness is the later outcome reflected in lower exposure, recurrence or loss severity and more timely response. This separation creates a clearer basis for future mediation and process research.

Third, the framework assigns digital enablement and governance to different parts of the causal sequence. Digital and analytical enablement is a first-stage amplifier because it affects the coverage and speed with which forensic expertise can identify and investigate anomalies. Governance, internal controls and ethical climate form a second-stage boundary condition because they affect whether uncomfortable findings are converted into actual control change. This distinction avoids treating every organisational factor as a general moderator and gives future empirical studies more precise relationships to test.

Practical And Policy Implications

For SME owners and managers, the starting point is to identify where access, authority and evidence are concentrated in one role. High-risk areas commonly include vendor creation and payment, payroll amendments, refunds, inventory write-offs, manual journals and related-party transactions. Those processes warrant selective forensic-style testing even when the individuals involved are trusted, because the control concern is access rather than presumed character.

SMEs should also build an evidence trail before an investigation is needed. Retaining source documents, documenting approvals, controlling system access, independently reconciling bank accounts and preserving transaction logs make later inquiry more reliable. These measures are not substitutes for forensic expertise, but they improve the quality of diagnostic evidence and reduce the ease with which records can be changed without trace.

Where an SME cannot justify an in-house forensic function, access can be created through external accountants, specialised investigators or periodic risk reviews. This is consistent with the capability perspective: what matters is the ability to mobilise appropriate expertise when risk warrants it. Professional capability and education remain recurring implementation issues in the forensic-accounting literature (Alshurafat et al., 2021; Guellim et al., 2024).

Digital investment should begin with the fraud problem rather than the software. An SME should first identify which transactions are high risk, what evidence would indicate an exception and who will evaluate the alert. Only then should it select an analytical tool. This sequence reduces the risk of paying for systems that produce a large volume of unexplained alerts without improving detection or control.

For policymakers, professional bodies and SME-support agencies, the framework suggests integrating fraud resilience into broader digitalisation and governance initiatives. Practical support can combine accounting-system training with access-control design, exception testing, evidence preservation, fraud escalation and guidance on when external forensic expertise is appropriate. The objective is not to turn every SME into an investigative unit, but to make basic forensic capability accessible and proportionate to business risk.

Limitations And Future Research

This paper is conceptual and does not estimate the size of the proposed relationships. The integrative review was designed to connect several literatures and does not claim exhaustive coverage. Although the final evidence base was deliberately verified and expanded, a future systematic review could use a preregistered protocol, database-specific search strings and formal quality appraisal to map the evidence more comprehensively.

The five propositions also require empirical testing. A Malaysian survey could operationalise forensic accounting capability, detection and diagnostic insight, preventive control remediation, digital and analytical enablement, governance and ethical climate, and financial fraud-control effectiveness as distinct constructs. The serial mechanism suggests a mediation structure, while P4 and P5 specify stage-specific moderation. Longitudinal designs would be particularly valuable because remediation and recurrence are difficult to evaluate at one point in time.

Case studies of SMEs that have experienced financial fraud could add process evidence that a cross-sectional survey cannot capture. Such studies could trace how the initial anomaly was identified, what evidence changed management's understanding, which control was subsequently redesigned and whether the same vulnerability reappeared. This would test the central claim that the value of forensic accounting depends on the movement from inquiry to organisational learning and corrective action.

Several contextual factors may also matter. Micro, small and medium-sized firms differ substantially in transaction volume and governance capacity; family ownership can affect willingness to challenge senior individuals; industry characteristics change the salience of cash, inventory, procurement and online transactions; and digital maturity may determine whether analytical tools improve inquiry or simply add complexity. Future research should test these factors without assuming that one configuration fits the entire SME population.

Finally, cost-effectiveness deserves direct attention. Forensic capability has practical value only when it is proportionate to risk. Comparative research on low-cost exception tests, periodic outsourced reviews and more formal in-house arrangements would help identify which configurations generate the greatest fraud-control benefit under different levels of SME complexity.

CONCLUSION

Financial fraud control in SMEs is more than a checklist of preventive procedures or a one-off investigation after a loss. The more useful question is whether the organisation can identify suspicious activity, understand

the weakness that enabled it, change that weakness and sustain a more resilient control environment. Forensic accounting contributes to this process when it is treated as an organisational capability rather than as a specialist label reserved for litigation.

The framework developed in this paper proposes a sequential mechanism: forensic accounting capability improves fraud detection and diagnostic insight; stronger diagnostic insight supports preventive control remediation; and effective remediation contributes to financial fraud-control effectiveness. Digital and analytical enablement strengthens the first relationship by expanding the reach of inquiry, while governance, internal controls and an ethical climate that supports challenge strengthen the second by determining whether findings are acted upon.

For Malaysian SMEs, the implication is deliberately practical. Effective forensic capability does not require every firm to maintain a large specialist department. It requires proportionate access to investigative expertise, usable evidence, disciplined follow-up and the willingness to redesign weak controls. Given the economic importance of Malaysian MSMEs, improving this capability can support firm-level financial integrity while also contributing to wider business resilience and stakeholder confidence.

ACKNOWLEDGEMENT

The author gratefully acknowledges UNITAR International University for its institutional support in facilitating this publication.

Ethical Considerations

This study is a conceptual review based on published literature and publicly available institutional reports. It did not involve human participants, animals or the collection of primary personal data; therefore, ethical approval was not required.

Conflict Of Interest

The author declares no conflict of interest in relation to this manuscript.

Data Availability

No new dataset was generated for this conceptual review. The sources used in the synthesis are identified in the reference list.

Declaration Of Generative Ai Assistance

Generative AI tools were used to support language refinement, structural editing and drafting assistance during preparation of this manuscript. The author independently reviewed and verified the arguments, citations, interpretations and final text and takes full responsibility for the scholarly content. Generative AI tools were not treated as authors, did not generate research data and were not relied upon as evidentiary sources.

REFERENCES

1. Airout, R. M., Abu Azam, S., & Airout, M. (2024). Bibliometric insights into the intellectual dynamics of forensic accounting research. *Cogent Business & Management*, 11(1), 2344748. <https://doi.org/10.1080/23311975.2024.2344748>
2. Alshurafat, H., Al Shbail, M. O., & Mansour, E. (2021). Strengths and weaknesses of forensic accounting: An implication on the socio-economic development. *Journal of Business and Socio-economic Development*, 1(2), 135-148. <https://doi.org/10.1108/JBSED-03-2021-0026>
3. Association of Certified Fraud Examiners. (2024). *Occupational fraud 2024: A report to the nations*. ACFE. <https://www.acfe.com/report-to-the-nations/2024/>

4. Awolowo, I. F., Ode, E., Abidoye, A., Ajao, O., & Jogunola, O. (2026). Cybersecurity assurance for SMEs: A conceptual framework integrating organizational culture, fraud risk management and forensic accounting. *Canadian Journal of Administrative Sciences / Revue Canadienne des Sciences de l'Administration*, 43(1), e70051. <https://doi.org/10.1002/cjas.70051>
5. Bakar, M. H. B. A., Kamal, M. E. M., & Ishak, M. S. (2023). The tendency for occupational fraud in Malaysian small medium enterprises and the effect of internal control, ethical culture and awareness on fraud. *International Journal of Academic Research in Business and Social Sciences*, 13(1), 1398-1424. <https://doi.org/10.6007/IJARBS/v13-i1/16293>
6. Committee of Sponsoring Organizations of the Treadway Commission, & Association of Certified Fraud Examiners. (2023). *Fraud risk management guide: Second edition - Executive summary*. COSO and ACFE. <https://www.acfe.com/fraud-resources/fraud-risk-tools---coso/fraud-risk-management-guide>
7. Department of Statistics Malaysia. (2026, July 30). Micro, small & medium enterprises (MSMEs) performance 2025. DOSM. <https://www.dosm.gov.my/portal-main/release-content/micro-small-medium-enterprises-msmes-performance-2025>
8. Guellim, N., Yami, N., Freihat, A. F., Alshurafat, H., Alkababji, M. W., Alzahrane, M., Gad, W. N.-E., Shaaban, M. S. I., & Mostafa, R. M. A. (2024). Evaluating the perceived value of forensic accounting: A systematic review method. *Discover Sustainability*, 5, 351. <https://doi.org/10.1007/s43621-024-00431-y>
9. Hasan, M. M. S., Abdul Latiff, A. R., & Zainl Abidin, Z. (2024). Impact of forensic accounting for strengthening company's internal audit systems in prevention and detection of financial fraud: A review. *European Journal of Business and Management*, 16(3), 50-62. <https://doi.org/10.7176/EJBM/16-3-07>
10. Hashim, H. A., Salleh, Z., Shuhaimi, I., & Ismail, N. A. N. (2020). The risk of financial fraud: A management perspective. *Journal of Financial Crime*, 27(4), 1143-1159. <https://doi.org/10.1108/JFC-04-2020-0062>
11. Howieson, B. (2018). What is the 'good' forensic accountant? A virtue ethics perspective. *Pacific Accounting Review*, 30(2), 155-167. <https://doi.org/10.1108/PAR-01-2017-0005>
12. Ibrahim, S., Idris, K. H., Lumat, Y., & Shimi, R. A. (2023). The effect of internal control on funds management by privately run Tahfiz schools in Klang Valley. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, 13(2), 239-248. <https://doi.org/10.6007/IJARAFMS/v13-i2/16759>
13. Isa, R. A. N. M., & Tazilah, M. D. A. K. (2026). Emerging forensic accounting technologies for fraud detection: A comprehensive scoping review. *Advanced International Journal of Business, Entrepreneurship and SMEs*, 8(28), 776-789. <https://doi.org/10.35631/AIJBES.828049>
14. Kaur, B., Sood, K., & Grima, S. (2022). A systematic review on forensic accounting and its contribution towards fraud detection and prevention. *Journal of Financial Regulation and Compliance*, 31(1), 60-95. <https://doi.org/10.1108/JFRC-02-2022-0015>
15. Murphy, P. R., & Free, C. (2016). Broadening the fraud triangle: Instrumental climate and fraud. *Behavioral Research in Accounting*, 28(1), 41-56. <https://doi.org/10.2308/bria-51083>
16. Nawawi, A., & Salin, A. S. A. P. (2018). Internal control and employees' occupational fraud on expenditure claims. *Journal of Financial Crime*, 25(3), 891-906. <https://doi.org/10.1108/JFC-07-2017-0067>
17. Nordin, S.-Z. S., Yap, B. W., Ng, K. H., Hashim, A., Rambeli, N., & Abdul Jalil, N. (2024). Predicting automobile insurance fraud using classical and machine learning models. *International Journal of Electrical and Computer Engineering*, 14(1), 911-921. <https://doi.org/10.11591/ijece.v14i1.pp911-921>
18. Oladejo, O. O. D., & Olorunsola, G. I. (2023). Forensic accounting and fraud prevention in owner-managed small and medium enterprises (SMEs) in Ogun State, Nigeria. *International Journal of Research and Innovation in Social Science*, 7(10), 477-490. <https://doi.org/10.47772/IJRISS.2023.701040>
19. Ozili, P. K. (2023). Forensic accounting research around the world. *Journal of Financial Reporting and Accounting*, 23(1), 128-153. <https://doi.org/10.1108/JFRA-02-2023-0106>

20. Singh, G. K., & Kumari, V. (2025). Research in forensic accounting and fraud detection: A systematic literature review. *International Journal of Accounting, Business and Finance*, 4(1), 53-65. <https://doi.org/10.55429/ijabf.v4i1.177>
21. Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333-339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
22. Sow, A. N., Basiruddin, R., Abdul Rasid, S. Z., & Md Husin, M. (2018b). Understanding fraud in Malaysian SMEs. *Journal of Financial Crime*, 25(3), 870-881. <https://doi.org/10.1108/JFC-08-2017-0077>
23. Sow, A. N., Basiruddin, R., Mohammad, J., & Abdul Rasid, S. Z. (2018a). 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>
24. Sutherland, E. H. (1949). *White collar crime*. Dryden Press.
25. Tiwari, R. K., & Debnath, J. (2017). Forensic accounting: A blend of knowledge. *Journal of Financial Regulation and Compliance*, 25(1), 73-85. <https://doi.org/10.1108/JFRC-05-2016-0043>
26. Torraco, R. J. (2016). Writing integrative literature reviews: Using the past and present to explore the future. *Human Resource Development Review*, 15(4), 404-428. <https://doi.org/10.1177/1534484316671606>