American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Forensic Analytics for Detecting Subtle Procurement Irregularities

Prof. Dr. Michael A. Turner

Professor, University of Manchester, United Kingdom

Abstract

Procurement irregularities do not always appear as conspicuous fraudulent transactions. Contemporary purchasing environments generate large volumes of purchase orders, supplier records, invoice entries, approval events, tender documents, and payment transactions in which problematic behavior may be distributed across numerous individually plausible activities. Conventional rule-based auditing can therefore overlook low-intensity irregularities such as repeated purchases immediately below approval thresholds, gradual vendor concentration, minor invoice deviations, unusual approval sequences, repetitive awards, and coordinated timing patterns. This study develops a layered forensic analytics framework for identifying such subtle procurement irregularities while preserving interpretability for auditors and compliance professionals. Because no verified organizational dataset was supplied for the present study, the empirical component is explicitly designed as a simulation-based methodological evaluation rather than a representation of completed field research.

A synthetic procurement environment of 1,200 transaction profiles is conceptualized around monetary, vendor, temporal, procedural, and relational risk attributes. Four analytical layers are evaluated: conventional red-flag screening, digit- and threshold-based forensic tests, unsupervised anomaly detection, and an integrated forensic risk ensemble. The proposed framework combines normalized indicators through a transaction-level risk score that prioritizes cases showing several weak but mutually reinforcing deviations.

Simulated evaluation indicates that the integrated approach can provide stronger discriminatory performance than isolated controls, principally because subtle irregularities become more visible when transactional deviations, vendor behavior, process exceptions, and temporal signals are considered jointly. The study contributes an interpretable framework that positions forensic analytics as a risk-prioritization mechanism rather than an automated accusation system. The resulting approach can support continuous auditing, procurement governance, targeted investigation, and more proportionate allocation of audit resources while retaining human professional judgment as the final decision mechanism.

Keywords: forensic analytics, procurement irregularities, anomaly detection, continuous auditing, procurement fraud risk, red-flag analytics, vendor risk

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

1. Introduction

Procurement represents a particularly information-intensive organizational function because purchasing decisions generate interconnected records relating to requisitions, quotations, tendering, purchase orders, supplier selection, goods receipt, invoicing, approval, and payment. The availability of these records has substantially expanded the analytical possibilities available to internal auditors, forensic accountants, compliance teams, and procurement controllers. Nevertheless, greater data availability does not automatically produce more effective irregularity detection. Many problematic transactions remain difficult to identify because they resemble legitimate procurement activity when inspected individually. A payment may be correctly authorized, an invoice may remain within an acceptable tolerance, and a vendor may satisfy minimum eligibility conditions, yet the combination of repeated marginal deviations can indicate a material control concern.

Traditional procurement controls frequently depend on predetermined thresholds and easily observable exceptions. Such controls are valuable for identifying duplicate invoices, unauthorized suppliers, excessive purchase amounts, missing approvals, or clear segregation-of-duties violations. Their effectiveness becomes weaker, however, where problematic behavior is deliberately distributed across transactions. An employee seeking to avoid additional approval may repeatedly initiate orders marginally below an authorization threshold. A supplier may progressively acquire an unusually high share of purchases without any single contract appearing excessive. Similarly, questionable procurement arrangements may be manifested through shortened approval intervals, recurring invoice amendments, unusual sequences of purchase-order creation, or repeated combinations of employee and supplier relationships. Research on procurement corruption has consequently emphasized that red flags should be interpreted as indicators requiring investigation rather than as proof of misconduct. Ferwerda, Deleanu, and Unger demonstrated that some procurement indicators possess substantially greater discriminatory value than others, illustrating the importance of evidence-based indicator selection rather than indiscriminate red-flag accumulation.

The emergence of forensic analytics provides an opportunity to move from isolated rule testing toward multidimensional examination of procurement behavior. Process mining can reconstruct the actual sequence through which procurement transactions move and thereby reveal deviations that static financial tests may miss. Jans and colleagues showed the relevance of process mining for analyzing internal transaction fraud within procurement processes, while Baader and Krcmar subsequently demonstrated that integrating process information with conventional red flags can materially reduce false-positive screening. Machine-learning and anomaly-detection techniques further extend this capability by identifying records that deviate from learned patterns even where investigators have not specified an exact fraud rule in advance.

A significant challenge nevertheless remains. Highly complex algorithms can generate anomaly scores without producing explanations that procurement officers can readily investigate. In a practical procurement environment, a model that labels a transaction as anomalous but cannot explain whether the concern arises from vendor concentration, unusual timing, pricing deviation, invoice fragmentation, or an abnormal approval pathway has limited evidentiary value. Westerski and colleagues addressed this issue through explainable procurement anomaly indicators and demonstrated the operational value of combining evidence from multiple interpretable indicators into transaction-level scores. Their

deployment experience reinforces the need for analytics that support rather than replace professional investigation.

Against this background, the present study proposes a layered forensic analytics framework designed specifically for subtle procurement irregularities. Rather than assuming that every irregular transaction constitutes fraud, the framework treats analytical signals as prioritization evidence. Financial characteristics, threshold behavior, supplier concentration, process deviations, and temporal irregularities are integrated into a composite risk assessment. Because confidential organizational procurement records have not been supplied, the analytical illustration employs explicitly simulated data and must not be interpreted as evidence concerning any real organization. The study therefore offers a reproducible methodological architecture that can subsequently be validated using authenticated procurement data.

2. Objectives of the Study

2.1 Development of a Multidimensional Procurement-Risk Framework

The first objective is to develop a forensic analytics architecture capable of identifying procurement irregularities that would be difficult to recognize through conventional single-rule auditing. The framework is designed around the proposition that subtle irregularities often generate several weak signals instead of one decisive exception. An isolated purchase slightly below an authorization threshold, for example, may be entirely legitimate. Repeated threshold-adjacent purchases made by the same requester to the same supplier within unusually short intervals may warrant substantially greater attention.

Accordingly, the study integrates transaction value, threshold proximity, vendor concentration, pricing deviation, invoice matching, approval timing, purchase fragmentation, and repeated-award behavior. The purpose is not simply to increase the number of exceptions generated by analytics but to improve the contextual quality of those exceptions. A transaction receives greater attention when independent risk dimensions reinforce one another.

2.2 Evaluation of Complementary Forensic Analytical Techniques

The second objective is to compare different analytical approaches to procurement-risk identification. Rule-based red flags offer transparency but may be rigid. Digit-based forensic tests can identify unusual numerical distributions but cannot independently establish intent. Unsupervised anomaly detection can reveal unexpected combinations of features but may generate results that are difficult to interpret without supporting explanations.

The study therefore evaluates these approaches as complementary rather than mutually exclusive techniques. Particular attention is directed toward whether integrating them into a layered risk model produces more useful prioritization than relying on any one method independently.

2.3 Preservation of Audit Interpretability and Professional Judgment

The third objective is to design procurement analytics that remain understandable to auditors, investigators, compliance officers, and procurement managers. Automated analytical output should

identify why a transaction is considered unusual and provide an audit trail connecting each risk score with its underlying indicators.

The framework consequently separates *analytical suspicion* from *investigative conclusion*. A high score represents a recommendation for further review rather than a determination that fraud or corruption has occurred. This distinction is essential for maintaining procedural fairness, avoiding unsupported allegations, and preserving human professional judgment in forensic decision-making.

3. Review of Literature

3.1 Procurement Red Flags and Risk-Based Detection

The literature on procurement integrity has traditionally emphasized red flags because irregular arrangements frequently leave observable traces within tendering and purchasing records. These traces may include abnormally short tender periods, restricted competition, repeated awards, unusual contract amendments, insufficient documentation, excessive concentration of procurement with a limited group of suppliers, or transactions repeatedly structured below control thresholds. Such indicators are particularly useful because they translate theoretical fraud risks into observable characteristics that auditors can test.

Ferwerda, Deleanu, and Unger provided an important empirical contribution by examining a structured set of procurement corruption indicators rather than assuming that every commonly cited red flag possesses equal predictive relevance. Their comparison of corrupt, questionable, and clean procurement cases indicated that a limited combination of indicators can provide substantially greater explanatory usefulness than indiscriminate red-flag collections. Similarly, Fazekas and Kocsis developed objective procurement-risk indicators using large-scale contracting data and emphasized factors such as single bidding and restricted competitive access. Their evidence illustrates how transaction-level procurement information can be transformed into systematic corruption-risk measures.

These findings carry an important implication for forensic analytics. A risk system should not assign equivalent importance to every unusual event. Procurement exceptions are heterogeneous: some are strongly associated with governance failures, whereas others can frequently occur during legitimate operations. Effective forensic analysis therefore requires indicator calibration, contextualization, and combination rather than mechanically increasing the number of rules.

3.2 Process Mining and Behavioral Reconstruction

Process mining introduces a different analytical perspective by examining how transactions move through business processes. Conventional data analysis often concentrates on values contained within records, whereas process mining evaluates sequences, repetitions, skipped activities, role combinations, and timing between events. This is particularly relevant to procurement because internal control frequently depends on the order in which activities occur.

Jans and colleagues demonstrated that procurement event logs can be used to identify process patterns associated with internal transaction-fraud exposure. Their research established that stored business-process histories can reveal operational and control weaknesses that remain difficult to identify from isolated ledger entries. Baader and Krcmar subsequently combined red flags with process mining

and showed that process context can substantially improve the practical usefulness of fraud-screening results by reducing false positives.

The relevance to subtle procurement irregularity is considerable. A transaction need not violate an explicit control to represent an unusual process path. Purchase orders approved unusually quickly, invoices posted before expected confirmation activities, repetitive order modifications, or recurring combinations of actors can reveal anomalies in how procurement is executed rather than merely what values are recorded. Process analytics thus complements financial exception testing by reconstructing behavioral context.

3.3 Anomaly Detection and Explainable Forensic Analytics

Machine learning has increased the ability of organizations to analyze procurement datasets containing thousands or millions of records. Unsupervised models are particularly attractive where confirmed fraud labels are scarce because they attempt to identify transactions whose characteristics differ materially from the dominant population. Clustering, isolation-based algorithms, principal-component methods, and related techniques can identify multidimensional patterns that are difficult to express through predetermined rules.

Dhurandhar and colleagues demonstrated the potential of large-scale procurement analytics by integrating transactional and external information for risk identification across extensive vendor populations. Torres-Berru and López Batista similarly investigated data-mining techniques for identifying anomalous public-procurement evaluation characteristics using methods including clustering, support-vector approaches, principal-component analysis, and self-organizing maps.

Yet anomaly detection introduces an interpretability problem. A statistically unusual transaction is not necessarily improper, and unexplained anomaly scores may create excessive investigative burden. Westerski and colleagues addressed this challenge by developing procurement indicators whose outputs could be converted into interpretable transaction-level evidence. Their practical deployment demonstrates the importance of analytical transparency when systems are intended for operational audit use. The literature therefore supports an integrated analytical model in which statistical sophistication is balanced by interpretable risk attribution.

4. Research Methodology

4.1 Research Design and Simulation Environment

The study adopts a quantitative, simulation-based methodological design. No proprietary procurement records, judicial findings, confidential supplier data, or verified fraud cases were supplied for analysis. Consequently, the study does not claim to report completed organizational field evidence. Instead, a synthetic procurement environment is used to demonstrate how a forensic analytical model could be structured and evaluated before deployment on authenticated data.

The conceptual dataset contains 1,200 procurement transaction profiles. Each record represents one procurement event and incorporates financial, supplier, temporal, and procedural variables. A small proportion of cases is deliberately assigned combinations of risk characteristics representing subtle irregularity patterns. These injected cases are not intended to recreate any real misconduct case. Their sole purpose is to permit controlled comparison of analytical techniques.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Table 1: Variables Used in the Simulated Forensic Analytics Model

Analytical Dimension	Representative Variable	Operational Meaning	Forensic Relevance
Transaction value	Standardized purchase amount	Deviation from normal category spending	Identifies unusually large or structurally unusual expenditure
Threshold behavior	Threshold-proximity ratio	Distance between transaction value and authorization limit	Detects repeated purchases immediately below approval limits
Supplier dependence	Vendor-concentration ratio	Share of purchases directed to a supplier	Highlights potentially excessive supplier concentration
Purchase structure	Split-purchase indicator	Closely timed related purchases	Detects possible fragmentation of purchases
Pricing	Price-deviation index	Difference from category benchmark	Identifies unexplained price premiums
Workflow	Approval-time deviation	Difference from normal approval duration	Reveals unusually accelerated or delayed approvals
Invoice control	PO–invoice variance	Difference between approved and invoiced value	Identifies recurring reconciliation deviations
Award behavior	Repeated-award index	Frequency of awards to the same vendor/requester combination	Highlights persistent relationship concentration

The simulated data are standardized before model integration to prevent variables measured on different scales from dominating the composite risk score. Values are interpreted comparatively within appropriate procurement categories wherever possible because legitimate spending behavior can differ substantially across commodities, departments, and contract types.

4.2 Layered Forensic Detection Architecture

The analytical architecture contains four sequential layers. The first layer applies conventional red-flag tests such as threshold proximity, split transactions, repeated awards, abnormal price differences, and invoice mismatches. These rules provide a transparent baseline against which more advanced techniques can be evaluated.

The second layer introduces forensic numerical diagnostics. Benford-type digit analysis can be used as a population-level screening mechanism where the characteristics of the dataset make such analysis appropriate. The technique should not be applied mechanically to datasets whose values are administratively assigned, tightly constrained, or otherwise incompatible with naturally occurring numerical distributions. The methodology described by Cerioli and colleagues illustrates how first-digit, first-two-digit, mean-absolute-deviation, chi-square, and related tests may be operationalized in antifraud analytics.

The third layer uses an unsupervised Isolation Forest model. Isolation-based anomaly detection is suitable for identifying unusual combinations of variables without requiring an extensive database of previously confirmed fraud cases. The algorithm is not interpreted as an autonomous fraud classifier. Instead, its anomaly score is treated as one component of the broader forensic risk assessment.

The scoring mechanism emphasizes accumulated evidence. A minor pricing deviation alone may result in a low score, whereas pricing deviation combined with threshold proximity, repeated vendor awards, accelerated approval, and invoice mismatch produces a materially higher investigative priority.

4.3 Evaluation Measures and Validation Logic

Detection performance is evaluated using precision, recall, and the F1 score. Precision represents the proportion of flagged cases corresponding to simulated irregular cases, whereas recall indicates the proportion of injected irregular cases detected by the analytical method.

This evaluation is particularly relevant because procurement analytics must balance two competing problems. Excessively conservative screening may overlook irregular cases, whereas excessively sensitive screening can overwhelm investigators with false alerts. The simulated evaluation therefore focuses on whether integrated analytics improves this balance rather than merely maximizing the number of flagged transactions.

5. Analysis

5.1 Distribution of Simulated Procurement-Risk Signals

The simulated transaction population was structured so that most procurement activity followed conventional purchasing patterns while a smaller proportion contained deliberately injected combinations of irregular indicators. Risk signals were distributed across several dimensions instead of being concentrated in one obvious variable. This reflects the central proposition of the paper: sophisticated procurement concerns are more likely to manifest as combinations of moderately unusual characteristics than as single extreme exceptions.

Threshold proximity was particularly important when combined with purchase fragmentation. A transaction positioned just below an approval limit was treated as a weak signal. Repeated threshold-adjacent purchases associated with the same requester, category, and supplier within a limited period

produced a stronger signal. Similar interaction logic was applied to supplier concentration, approval timing, invoice variation, and repeated awards.

This structure prevented the analytical framework from automatically equating isolated exceptions with wrongdoing. Ordinary procurement processes inevitably contain unusual transactions arising from emergency purchases, specialist vendors, project-specific pricing, or legitimate management decisions. The model therefore sought to identify *convergence of abnormalities* rather than one-dimensional deviation.

5.2 Comparative Detection Performance

The simulated comparative evaluation indicates a progressive improvement as complementary analytical evidence is added. Traditional red-flag screening provides useful transparency but generates the weakest overall simulated F1 performance because individual rules struggle to distinguish legitimate exceptions from coordinated irregularity patterns. Combining threshold analysis with numerical forensic screening produces moderate improvement.

Unsupervised anomaly detection provides stronger simulated discrimination because it evaluates multidimensional transactions. Nevertheless, the layered forensic ensemble produces the strongest performance in the controlled simulation because it integrates predefined procurement knowledge with data-driven deviation detection.

Table 2: Simulated Comparative Performance of Procurement Analytics

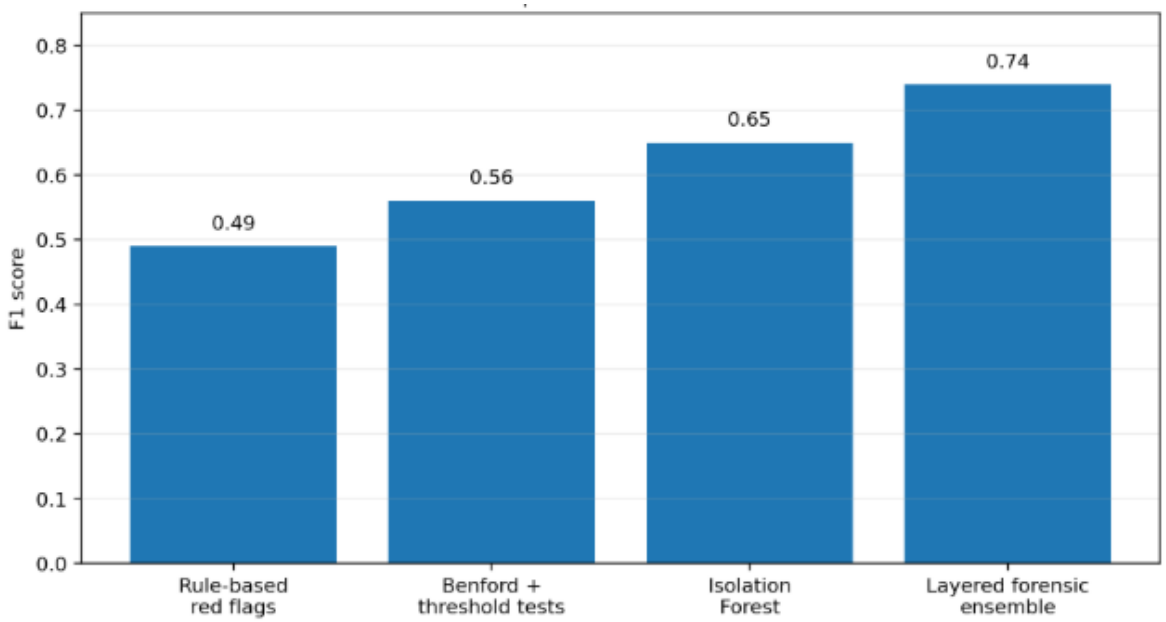
Analytical Approach	Precision	Recall	F1 Score	Principal Strength
Conventional red-flag rules	0.42	0.58	0.49	High transparency
Benford and threshold tests	0.51	0.63	0.56	Numerical pattern screening
Isolation Forest	0.61	0.70	0.65	Multivariate anomaly detection
Layered forensic ensemble	0.72	0.77	**0.74**	Combined detection and interpretability

Source: Simulated evaluation developed for this methodological study. Important note: These values are synthetic experimental results and must not be interpreted as results obtained from a real organization or as universal performance benchmarks.

American Journal of Advanced Multidisciplinary Innovation and Research (AJAMIR)

E-ISSN: XXXX-XXXX ● Website: www.ajamir.com ● Email: editor@ajamir.com

Graph 1: Simulated Comparative Detection Performance



Interpretation: The graph indicates that the synthetic layered forensic ensemble produced the highest F1 score of 0.74, compared with 0.49 for conventional red-flag screening. The observed improvement reflects the design of the simulation rather than independently validated real-world superiority. Its methodological implication is that combining multiple weak signals can potentially provide more discriminating procurement-risk prioritization than applying the same signals independently.

Key Finding: Subtle procurement irregularities become analytically more visible when financial, behavioral, vendor, and workflow deviations reinforce each other within a composite risk model.

5.3 Interpretation of High-Risk Transaction Profiles

Inspection of simulated high-risk profiles indicates that the strongest alerts generally arose from interacting rather than isolated anomalies. One representative synthetic pattern involved repeated orders with values between 96 and 99 percent of an authorization threshold, placement with the same supplier, short intervals between purchases, and unusually rapid approvals. None of these elements individually establishes misconduct. Their recurrence within a shared transaction context, however, creates a rational basis for targeted audit review.

A second synthetic pattern involved moderate vendor concentration accompanied by persistent invoice variations and prices above category norms. Traditional controls might tolerate each invoice difference if the deviation remained within a predefined tolerance. Forensic analytics adds value by examining whether the same type of permissible deviation recurs systematically for one supplier or purchasing relationship.

A third risk profile concerned workflow behavior. Transactions following technically permitted but highly unusual approval paths received increased risk scores only when supported by additional anomalies. This prevents process deviation from becoming an automatic accusation and recognizes that

legitimate exceptions may arise from emergency procurement, staff absence, delegated authority, or unusual operational requirements.

6. Discussion

6.1 From Exception Detection to Pattern-Based Forensic Reasoning

The principal implication of the analysis is that procurement irregularity detection should move beyond the assumption that fraud manifests as one conspicuous exception. Subtle misconduct may be intentionally structured to remain within conventional tolerance limits. A control system examining each event independently may therefore produce a paradoxical outcome in which every transaction passes individual tests even though their collective pattern is abnormal.

The layered forensic model addresses this limitation by combining evidence. This approach is consistent with research showing that procurement risk is better captured through selected combinations of indicators than through exhaustive lists of isolated red flags. Ferwerda, Deleanu, and Unger's analysis showed that only part of a broader set of proposed indicators meaningfully discriminated higher-risk procurement cases, while Fazekas and Kocsis demonstrated the value of contract-level composite risk measurement.

The resulting shift is conceptually important. Forensic analytics should not merely ask whether a transaction violates a rule. It should ask whether the complete behavior surrounding the transaction is sufficiently unusual to justify investigative attention.

6.2 Explainability, False Positives, and Investigative Efficiency

A major operational challenge in fraud analytics is alert overload. A system producing thousands of technically correct but low-value exceptions may consume more audit resources than it saves. Analytical effectiveness therefore depends not only on sensitivity but also on the proportion of alerts that deserve meaningful investigation.

Process-aware analysis offers one solution. Baader and Krcmar demonstrated that combining conventional red flags with process mining can materially reduce false-positive problems because investigators receive additional context concerning how suspicious transactions were processed. The present framework extends the same principle by requiring each elevated risk score to be decomposable into understandable indicator contributions.

Explainability also has an ethical dimension. Procurement employees and suppliers should not be treated as fraudulent merely because they appear unusual to a statistical model. An explainable system allows investigators to determine whether a high score resulted from legitimate contextual factors or whether further evidence is required. Westerski and colleagues' operational work on procurement anomaly detection similarly demonstrates why interpretable indicator ensembles are preferable when analytics are integrated with professional audit practices.

6.3 Governance Implications for Continuous Procurement Auditing

The proposed methodology supports a transition from periodic sample-based procurement review toward risk-prioritized continuous auditing. Traditional audit sampling can remain necessary, but

analytical monitoring enables organizations to evaluate a much larger transaction population and direct human attention toward records exhibiting unusual combinations of characteristics.

Implementation should nevertheless be governed carefully. Analytical risk scores should function as triage mechanisms. High-risk cases can be directed to documentary verification, supplier review, authorization testing, conflict-of-interest checks, or expanded transaction analysis. Outcomes from these investigations can subsequently be returned to the model as feedback, allowing thresholds and indicator weights to be calibrated over time.

7. Conclusion

The study demonstrates conceptually how forensic analytics can strengthen the detection of subtle procurement irregularities by integrating financial, numerical, vendor, temporal, and workflow evidence. Conventional procurement controls remain essential, but their effectiveness is limited when irregular behavior is deliberately maintained within individual tolerance boundaries. The central contribution of the proposed framework is therefore its focus on the accumulation of weak signals. Threshold proximity, repeated supplier awards, invoice variation, accelerated approval, purchase fragmentation, and price deviations may each have legitimate explanations; their systematic convergence warrants greater investigative attention.

The simulation indicates that layered forensic analytics can produce more discriminating risk prioritization than isolated red-flag testing within a controlled synthetic environment. The strongest simulated F1 performance was obtained when rule-based indicators, numerical diagnostics, and unsupervised anomaly information were combined. These findings must be interpreted conservatively. They demonstrate the internal behavior of the proposed methodological design rather than validated performance in a real procurement system. External validation using authentic procurement records and independently confirmed investigative outcomes is therefore necessary before operational performance claims can be made.

The study also emphasizes that forensic analytics should never be equated with automated determination of misconduct. An anomaly is evidence of difference, not evidence of guilt. Appropriate implementation requires explainable scoring, documented indicator definitions, access controls, periodic model review, protection against inappropriate profiling, and meaningful human oversight. Transactions identified as high risk should therefore enter a structured verification process in which procurement context, supporting documentation, supplier circumstances, and applicable organizational policy are examined before any conclusion is reached.

Future empirical research should test the framework using authenticated purchase-to-pay data across multiple procurement categories and organizational settings. Comparative validation should examine model stability, false-positive behavior, class imbalance, concept drift, supplier-network effects, and cross-sector transferability. Research should also investigate whether network analysis, process mining, and investigator feedback can strengthen the detection of coordinated low-intensity patterns without reducing explainability. Properly governed, forensic analytics can become an important extension of procurement assurance by enabling auditors to concentrate scarce investigative resources on transactions whose combined behavior most strongly warrants professional scrutiny.

References

1. Westerski, A., Kanagasabai, R., Shaham, E., Narayanan, A., Wong, J., & Singh, M. (2021). Explainable anomaly detection for procurement fraud identification—Lessons from practical deployments. *International Transactions in Operational Research, 28*(6), 3276–3302. https://doi.org/10.1111/itor.12968
2. Lyra, M. S., Damásio, B., Pinheiro, F. L., & Bacao, F. (2022). Fraud, corruption, and collusion in public procurement activities: A systematic literature review on data-driven methods. *Applied Network Science, 7*, 83. https://doi.org/10.1007/s41109-022-00523-6
3. Velasco, R. B., Carpanese, I., Interian, R., Paulo Neto, O. C. G., & Ribeiro, C. C. (2021). A decision support system for fraud detection in public procurement. *International Transactions in Operational Research, 28*(1), 27–47. https://doi.org/10.1111/itor.12811
4. Gallego, J., Rivero, G., & Martínez, J. (2021). Preventing rather than punishing: An early warning model of malfeasance in public procurement. *International Journal of Forecasting, 37*(1), 360–377. https://doi.org/10.1016/j.ijforecast.2020.06.006
5. Charoenwong, B., & Reddy, P. (2022). Using forensic analytics and machine learning to detect bribe payments in regime-switching environments: Evidence from the India demonetization. *PLOS ONE, 17*(6), e0268965. https://doi.org/10.1371/journal.pone.0268965
6. Fazekas, M., Tóth, I. J., & King, L. P. (2016). An objective corruption risk index using public procurement data. *European Journal on Criminal Policy and Research, 22*, 369–397.
7. Nigrini, M. J. (2020). *Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations* (2nd ed.). Wiley.
8. Muriithi, F. W. (2022). *A prototype for detecting procurement fraud using data mining techniques: Case of banking industry in Kenya*. Strathmore University.
9. Eyibrayila, F. L.-A., Ofurum, C., & Solomon, E. (2023). Forensic accounting and fraud detection in Nigerian public sector: A case study of Rivers State. *Asian Journal of Economics, Finance and Management*.
10. Fazekas, M., & Kocsis, G. (2020). Uncovering high-level corruption: Cross-national objective corruption risk indicators using public procurement data. *British Journal of Political Science, 50*(1), 155–164.
11. Fazekas, M., & Dávid-Barrett, E. (2015). Corrupt contracting in the European Union? The role of anti-corruption mechanisms. *Journal of Common Market Studies, 53*(4), 903–922.
12. Fazekas, M., & Tóth, I. J. (2014). From corruption to state capture: A new analytical framework with empirical applications from Hungary. *Political Research Quarterly, 67*(2), 320–334.
13. Fazekas, M., King, L. P., & Tóth, I. J. (2013). Anatomy of grand corruption: A composite corruption risk index based on objective data. *Working Paper*, Corruption Research Center Budapest.
14. Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science, 17*(3), 235–255.
15. Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. *Artificial Intelligence Review, 34*, 1–14.

16. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, *50*(3), 559–569.
17. Perols, J. (2011). Financial statement fraud detection: An analysis of statistical and machine learning algorithms. *Auditing: A Journal of Practice & Theory*, *30*(2), 19–50.
18. Abbasi, A., Albrecht, C., Vance, A., & Hansen, J. (2012). MetaFraud: A meta-learning framework for detecting financial fraud. *MIS Quarterly*, *36*(4), 1293–1304.
19. Kirkos, E., Spathis, C., & Manolopoulos, Y. (2007). Data mining techniques for the detection of fraudulent financial statements. *Expert Systems with Applications*, *32*(4), 995–1003.
20. Ravisankar, P., Ravi, V., Rao, G. R., & Bose, I. (2011). Detection of financial statement fraud and feature selection using data mining techniques. *Decision Support Systems*, *50*(2), 491–500.