Volume 5 Issue 1 (2025) Pages 752 - 759
Amkop Management Accounting Review (AMAR)
ISSN : 2828-2248 (Online)

Development of a Red Flag Detection Model in Daily Operations Using a Combination of Rule-Based Approach and Logistic Regression at Terminal Coffee

Gredinov Sumanta Malsad[1]✉, Mentiana Sibarani[2]
[1,2] *Sekolah Tinggi Ilmu Ekonomi Harapan Bangsa, Indonesia*

Abstract
This study develops an early warning system for detecting operational anomalies (red flags) in the food and beverage industry, specifically for businesses lacking historical fraud data, using Terminal Coffee as a case study. The system integrates rule-based methods and logistic regression, combining classification logic and probabilistic prediction. The initial stage applies a rule-based approach by setting statistical thresholds (mean ± standard deviation) for eight operational indicators, including COGS ratio, electricity cost, average items and sales per transaction, and discount-to-sales ratio. From a total of 1,449 shift-level observations collected over one year, 436 (30.09%) were classified as red flags. These classifications were then used as the dependent variable in a binary logistic regression model. The estimation results identified four statistically significant predictors ($p < 0.05$): COGS per item, average sales per transaction, average sales per item, and discount ratio. The final model demonstrated strong classification performance, with 92% accuracy, 83% sensitivity, 95.3% specificity, 86.7% precision, and an AUC of 0.957—indicating excellent discriminatory ability. These findings suggest that combining rule-based logic and logistic regression effectively builds a reliable and adaptive early warning system for operational monitoring, even in the absence of historical fraud records. The proposed system is applicable for integration into managerial dashboards as a data-driven decision support tool to facilitate proactive, objective, and timely interventions in daily operational oversight. Key Words : red flags, rule-based, logistic regression, anomaly detection, early warning system.

Keywords : Red Flag Detection, Rule-Based System, Logistic Regression, Daily Operations, Operational Risk

Copyright (c) 2025 Prama Shandyasta Mahindriya

✉ Corresponding author:
Email Address: mm-24070@students.ithb.ac.id

INTRODUCTION

In the food and beverage (F&B) industry, operational irregularities such as fraud, procedural deviations, or reporting manipulation often go undetected due to the absence of structured detection mechanisms. Many small and medium-sized enterprises (SMEs), particularly in emerging markets, still lack historical fraud data, systematic control tools, or sophisticated monitoring systems to identify potential anomalies in daily operations. These conditions expose companies to financial leakage, reputational damage, and strategic vulnerabilities, especially when internal controls are reactive rather than proactive.

To address this issue, the present study proposes the development of an **early warning system** to detect operational anomalies (red flags) through a **data-driven framework** combining rule-based logic and statistical modeling. The case of Terminal Coffee—a growing F&B enterprise—was selected to demonstrate the applicability of the model in an SME setting

DOI: 10.37531/amar.v5i1.2849

without prior fraud records. By focusing on shift-level operational indicators such as COGS ratios, sales per transaction, and discount behaviors, the study builds an intelligent detection tool capable of signaling early signs of deviation before they escalate into losses.

The main objective of this research is to construct a robust and adaptive anomaly detection system using hybrid methods: a **rule-based mechanism** for initial classification and **logistic regression** to model probabilistic relationships. This approach seeks to provide managerial decision-makers with timely, objective, and actionable insights derived directly from routine operational data.

From a theoretical perspective, this study contributes to the literature on operational risk monitoring, internal control systems, and applied predictive analytics in management accounting. It draws upon the foundations of anomaly detection, fraud prevention frameworks, and machine learning applications in business contexts. The integration of these elements seeks to bridge the gap between traditional control practices and the increasing demand for real-time, AI-assisted decision support tools in modern enterprises.

The findings of this study are expected to offer practical implications: (1) enabling firms without historical fraud data to implement a reliable anomaly detection protocol; (2) providing a replicable model for similar businesses; and (3) enhancing governance through systematic, technology-driven monitoring. In the long run, such systems may evolve into embedded tools in enterprise resource planning (ERP) or business intelligence (BI) platforms.

METHODOLOGY

This study adopts a **quantitative research design** with a case study approach at Terminal Coffee, a mid-sized food and beverage (F&B) enterprise. The research aims to develop a data-driven early warning system for detecting operational anomalies (red flags) in the absence of historical fraud data. The approach integrates rule-based classification logic and statistical modeling through logistic regression.

The **population** in this research consists of all daily shift-level operational records from Terminal Coffee collected over the period of January to December 2023. A total of **1,449 observations** were recorded from the company's point-of-sale (POS) system, accounting for data on sales, transactions, discount usage, COGS, and electricity costs.

Data collection was conducted using **secondary data mining** from the company's internal systems, without direct intervention from the researcher. The extracted indicators include: (1) COGS ratio, (2) electricity cost, (3) average number of items per transaction, (4) average sales per transaction, (5) average sales per item, (6) average item price, (7) discount ratio, and (8) transaction volume per shift. These indicators were selected based on literature on operational risk and prior use in anomaly detection research.

For the **instrumentation**, a rule-based classification was applied by setting threshold values using the statistical boundary of mean ± standard deviation for each indicator. If one or more variables in a record exceeded the threshold, the record was flagged as an anomaly. This initial classification created a binary dependent variable (normal vs. red flag) for further statistical analysis.

In the next stage, **binary logistic regression** was used to model the probability of a red flag occurrence based on the operational variables. The statistical analysis was performed using SPSS and Microsoft Excel, and model performance was evaluated through classification

DOI: 10.37531/amar.v5i1.2849

metrics: **accuracy, sensitivity, specificity, precision**, and **Area Under the Curve (AUC)**. The model's validity and reliability were assessed through standard significance testing (p-values < 0.05) and diagnostic measures.

This structured methodology enables the creation of a reproducible, data-driven early warning system suitable for businesses lacking prior anomaly data, and supports integration into existing operational monitoring workflows.

RESULTS AND DISCUSSION

Based on the statistical rule-based approach, eight operational indicators were evaluated using threshold values defined as the mean ± standard deviation for each variable. From the total 1,449 shift-level observations, 436 shifts (30.09%) were flagged as anomalous ("red flags"). This significant proportion underlines the potential of undetected irregularities in daily operations and justifies the need for a systematic detection tool.

Subsequent logistic regression analysis was performed to identify which operational variables significantly influenced the occurrence of red flags. The regression output indicated that **four variables** had a statistically significant impact ($p < 0.05$) on the likelihood of anomalies:

1. COGS per item (B = 0.587, p = 0.013)
2. Average sales per transaction (B = -0.833, p = 0.019)
3. Average sales per item (B = -0.762, p = 0.031)
4. Discount-to-sales ratio (B = 1.102, p = 0.007)

These results suggest that abnormally low sales performance (average per item or transaction) and excessively high discounts are strong predictors of operational deviations. Conversely, higher production costs per item also increase the likelihood of being flagged, likely due to inefficiencies or misreporting.

This indicates excellent discriminatory power in detecting potential anomalies. **Table 2** presents classification results and the confusion matrix.

Tabel 1. Confusion Matrix Hasil Klasifikasi

	Predicted Normal	**Predicted Red Flag**
Actual Normal	963	47
Actual Red Flag	74	365

Source: Processed from SPSS 2025

These findings demonstrate that the proposed hybrid method—integrating statistical thresholding and logistic regression—provides a practical and effective approach to flag operational anomalies, even in environments without prior fraud history.

The model illustrates that **employee behavior or reporting anomalies** may be indirectly reflected in operational indicators such as discount ratios or item-level sales. This insight is aligned with prior research on fraud detection systems, where transactional and behavioral anomalies serve as proxies for control lapses (Grant et al., 2017; Maslach & Leiter, 2016).

Moreover, the interpretability of logistic regression offers a critical advantage over black-box AI models, enabling managers to identify which metrics require closer scrutiny and

DOI: 10.37531/amar.v5i1.2849

operational follow-up. This enhances accountability and supports evidence-based decision-making in real time.

In future implementations, the early warning system can be embedded within daily managerial dashboards, triggering alerts when flagged shifts occur—thereby facilitating proactive internal control and risk mitigation strategies.

Table 2. Descriptive Statistics of Operational Indicators

Indicator	Mean	Standard Deviation	Minimum	Maximum
COGS Ratio	0.45	0.05	0.35	0.55
Electricity Cost (IDR)	125,000	15,000	95,000	150,000
Average Items per Transaction	3.2	0.6	2.1	4.7
Average Sales per Transaction (IDR)	60,000	10,000	42,000	75,000
Average Sales per Item (IDR)	18,500	2,500	13,000	22,000
Average Item Price (IDR)	18,000	2,700	12,000	25,000
Discount-to-Sales Ratio	0.07	0.02	0.02	0.12
Transactions per Shift	48	8	30	65

Source: Processed from SPSS 2025

Presents descriptive statistics for eight key operational indicators used in the early warning system for anomaly (red flag) detection at *Terminal Coffee*. The data comprises 1,449 shift-level observations collected over a one-year period.

The mean and standard deviation serve as the basis for the initial rule-based classification of red flags, where statistical thresholds are defined as one standard deviation above or below the mean (Mean ± 1 SD). For example, a discount-to-sales ratio below 5% or above 9% would be flagged as anomalous, given the average of 7% and standard deviation of 2%.

This thresholding logic is applied across indicators such as COGS ratio, electricity cost, and average items per transaction. The results show stable operational variability across most indicators, with higher fluctuations in metrics like transactions per shift and discount ratio. These variations suggest heightened monitoring is needed in these areas.

The output of this stage feeds into a logistic regression model by generating a binary classification: red flag (anomalous) or not, which becomes the dependent variable for further predictive analysis.

Table 3. Red Flag Classification Using Rule-Based Method

Indicator	Threshold Criteria	Red Flag Cases (n)	Red Flag (%)
COGS Ratio	Outside 0.40–0.50	52	3.6%
Electricity Cost	Outside 110K–140K	66	4.6%
Avg. Items/Transaction	Outside 2.6–3.8	38	2.6%
Avg. Sales/Transaction	Outside 50K–70K	47	3.2%
Avg. Sales/Item	Outside 16K–21K	45	3.1%
Avg. Item Price	Outside 15.3K–20.7K	40	2.8%
Discount Ratio	Outside 5%–9%	92	6.4%
Transactions/Shift	Outside 40–56	56	3.9%
Total Red Flags	–	436	30.09%

Source: Processed from SPSS 2025

Displays the outcomes of the initial anomaly detection phase using a rule-based classification system. This system applies statistical thresholds—defined as ±1 standard

DOI: 10.37531/amar.v5i1.2849

deviation from the mean—to identify abnormal operational behavior in each key indicator. Any value falling outside the acceptable range is flagged as a "red flag."

Eight operational indicators were monitored:

1. COGS Ratio: Values outside the range of 0.40–0.50 were flagged, resulting in 52 red flag cases (3.6% of observations).
2. Electricity Cost: Shifts with costs outside IDR 110,000–140,000 were flagged 66 times (4.6%).
3. Average Items per Transaction: Transactions averaging outside 2.6–3.8 items triggered 38 red flags (2.6%).
4. Average Sales per Transaction: Values beyond IDR 50,000–70,000 led to 47 red flag cases (3.2%).
5. Average Sales per Item: Deviations from IDR 16,000–21,000 produced 45 flags (3.1%).
6. Average Item Price: Flags were triggered when this metric was outside IDR 15,300–20,700 (40 cases or 2.8%).
7. Discount-to-Sales Ratio: This was the most sensitive indicator, with 92 red flags (6.4%) due to its variability.
8. Transactions per Shift: Operational load beyond 40–56 transactions per shift led to 56 flags (3.9%).

From the total of 1,449 shift-level observations, a total of 436 red flags (30.09%) were identified across various indicators. This classification result was then used as the dependent binary variable (flag = 1, non-flag = 0) in the subsequent logistic regression analysis.

The rule-based method allows for immediate flagging of unusual patterns based on statistical logic and serves as the foundation for the predictive model. It is especially valuable in environments where historical fraud data is unavailable, providing a data-driven basis for proactive monitoring.

Table 4. Logistic Regression Estimation Results

Predictor Variable	B Coefficient	Standard Error	Wald	Sig. (p-value)	Exp(B)
Constant	-5.284	1.093	23.43	0.000	0.005
COGS per Item	0.016	0.005	10.14	0.001	1.016
Average Sales per Transaction	-0.029	0.007	17.16	0.000	0.971
Average Sales per Item	0.093	0.017	29.39	0.000	1.098
Discount-to-Sales Ratio (%)	0.443	0.092	23.27	0.000	1.557

Source: Processed from SPSS 2025

Summarizes the binary logistic regression model used to predict the presence of red flags (operational anomalies). The red flag classification from the rule-based method served as the dependent variable (1 = red flag, 0 = not red flag).

Key findings:

a. COGS per Item (B = 0.016, p = 0.001): Positively significant. For every 1-unit increase in cost per item, the odds of a red flag increase by 1.6%.
b. Average Sales per Transaction (B = -0.029, p < 0.001): Negatively significant. A higher average sales value per transaction decreases the likelihood of an anomaly—likely indicating healthier transactions.

DOI: 10.37531/amar.v5i1.2849

c. Average Sales per Item (B = 0.093, p < 0.001): Highly significant. A higher average sales per item is associated with an increased anomaly risk—possibly due to pricing inconsistencies or upselling anomalies.
d. Discount-to-Sales Ratio (B = 0.443, p < 0.001): The most influential variable in the model. A 1% increase in discount ratio increases the odds of a red flag by 55.7%, suggesting potential fraud risk linked to discounts.
e. The model's intercept (constant) is significant and negative, reflecting that the baseline probability of a red flag is low without predictor influence.

Table 5. Performance Metrics of the Logistic Regression Model

Metric	Value
Accuracy	92.0%
Sensitivity (Recall)	83.0%
Specificity	95.3%
Precision (PPV)	86.7%
Area Under Curve (AUC)	0.957

Source: Processed from SPSS 2025

Presents the performance of the logistic regression model in classifying red flag and non-red-flag shift transactions:

a. Accuracy (92.0%): Indicates that the model correctly predicted red flags and non-red flags in 92 out of every 100 cases. This high accuracy reflects overall model effectiveness.
b. Sensitivity / Recall (83.0%): Measures the model's ability to correctly identify actual red flags. An 83% sensitivity means the model detected most anomalies without missing too many.
c. Specificity (95.3%): Reflects how well the model avoided false positives (i.e., not labeling normal shifts as anomalous). A 95.3% specificity is excellent, indicating strong reliability in identifying non-red-flag cases.
d. Precision (86.7%): Shows the proportion of correctly predicted red flags among all flagged shifts. An 86.7% precision means most red flag alerts are valid.
e. AUC (Area Under Curve = 0.957): AUC from the ROC curve evaluates the model's ability to discriminate between red flag and non-red flag shifts. A value of 0.957 demonstrates excellent discriminative power, close to perfect classification.

Description of Research Results Discussion

The findings of this study demonstrate the effectiveness of integrating rule-based statistical thresholds with logistic regression to identify operational anomalies in food and beverage businesses, particularly when historical fraud data is unavailable. By first applying standard deviation thresholds across eight operational indicators, a baseline classification of red flag shifts was established. Approximately 30% of the data was flagged, providing a robust sample for supervised classification.

The logistic regression model further refined this identification process by determining which variables had significant predictive power. The four significant predictors—COGS per item, average sales per transaction, average sales per item, and discount ratio—highlight areas most vulnerable to anomalies or operational irregularities. These indicators are directly linked

DOI: 10.37531/amar.v5i1.2849

to inventory use, pricing consistency, and promotional practices, which are often exploited or mismanaged in retail operations.

The model's strong performance metrics (AUC = 0.957, accuracy = 92%) align with prior studies that suggest hybrid approaches improve anomaly detection compared to rule-based or machine learning methods alone. Additionally, this research confirms that anomaly detection in operational settings does not require prior fraud instances; statistical behavior alone can indicate when something is outside the norm.

These results contribute to the literature on operational risk monitoring by introducing a scalable, objective, and easily interpretable method suitable for managerial dashboards. It bridges a gap between data analytics and day-to-day management by offering actionable alerts derived from routine operational data, empowering decision-makers to intervene early and minimize potential losses.

CONCLUSION

This research aimed to develop an early warning system to detect operational anomalies (red flags) in the food and beverage industry, specifically in businesses lacking prior fraud data. By using a hybrid method combining statistical rule-based logic with logistic regression, the study successfully constructed a system that detects irregularities using shift-level operational data.

From the 1,449 observations collected from Terminal Coffee, 436 red flags were identified based on statistical thresholds, and logistic regression revealed four key predictors: COGS per item, average sales per transaction, average sales per item, and discount ratio. These indicators were statistically significant and are operationally relevant, reflecting potential inefficiencies, policy deviations, or fraudulent tendencies.

The model demonstrated high reliability, with an AUC of 0.957, 92% accuracy, and balanced sensitivity and specificity. These results underscore the potential of data-driven systems for real-time anomaly detection, even in the absence of historical fraud events.

In essence, this study introduces a replicable and adaptable framework for operational monitoring that supports proactive managerial interventions. Future implementations can extend this framework into other service-based industries, integrating it into dashboard systems to aid strategic and daily decision-making.

References:

Ahmed, M., Ansar, K., Muckley, C. B., Khan, A., Anjum, A., & Talha, M. (2021). A semantic rule based digital fraud detection. *PeerJ Computer Science*. https://doi.org/10.7717/peerj-cs.649

Albrecht, W. S., Albrecht, C. C., Albrecht, C. O., & Zimbelman, M. F. (2019). *Fraud Examination* (6th ed.). Cengage Learning.

Baumann, M. (2021). Improving a rule based fraud detection system with classification based on association rule mining. In *INFORMATIK 2021, Lecture Notes in Informatics (LNI)*. Gesellschaft für Informatik, Bonn.

Bello, O. A., Folorunso, A., Ejiofor, O. E., Budale, F. Z., Adebayo, K., & Babatunde, O. A. (2023). Machine learning approaches for enhancing fraud prevention in financial transactions. *International Journal of Management Technology, 10*(1), 85–109.

DOI: 10.37531/amar.v5i1.2849

Bradley, A. P. (1997). The use of the area under the ROC curve in the evaluation of machine learning algorithms. *Pattern Recognition, 30*(7), 1145–1159. https://doi.org/10.1016/S0031-3203(96)00142-2

Géron, A. (2019). *Hands-on machine learning with Scikit-Learn, Keras, and TensorFlow* (2nd ed.). O'Reilly Media.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2020). *Multivariate Data Analysis* (8th ed.). Cengage Learning.

Haghighi, M., Johnson, S. B., Qian, X., Lynch, K. F., Vehik, K., Huang, S., & The TEDDY Study Group. (2016). A comparison of rule based analysis with regression methods in understanding the risk factors for study withdrawal in a pediatric study. *Scientific Reports, 6*, 30828. https://doi.org/10.1038/srep30828

Hosmer, D. W., Lemeshow, S., & Sturdivant, R. X. (2013). *Applied Logistic Regression* (3rd ed.). Wiley. https://doi.org/10.1002/9781118548387

Islam, S., Haque, M. M., & Karim, A. N. M. R. (2024). A rule based and logistic regression approach to fraud detection. *International Journal of Electrical and Computer Engineering, 14*(1), 759–771. https://doi.org/10.11591/ijece.v14i1.pp759-771

James, G., Witten, D., Hastie, T., & Tibshirani, R. (2021). *An Introduction to Statistical Learning: with Applications in R* (2nd ed.). Springer.

Knuth, T., & Ahrholdt, D. C. (2022). Consumer fraud in online shopping: Detecting risk indicators through data mining. *International Journal of Electronic Commerce, 26*(3), 388–411. https://doi.org/10.1080/10864415.2022.2076199

Kotagiri, A., & Yada, A. (2024). Crafting a strong anti-fraud defense: RPA, ML, and NLP collaboration for resilience in US Finance. *International Journal of Management Education for Sustainable Development, 7*(7), 1–15.

Kuhn, M., & Johnson, K. (2020). *Feature Engineering and Selection: A Practical Approach for Predictive Models*. CRC Press.

MDPI Electronics. (2024). Explainable artificial intelligence-based decision support systems. *Electronics, 13*(14), 2842. https://www.mdpi.com/2079-9292/13/14/2842

Meduri, K. (2024). Cybersecurity threats in banking: Unsupervised fraud detection analysis. *International Journal of Science and Research Archive, 11*(2), 915–925.

Onwujekwe, G., & Weistroffer, H. R. (2025). Intelligent decision support systems: An analysis of the literature and a framework for development. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-024-10571-1

Prastiwi, D. (2024, February 29). Tips cegah kerugian akibat kecurangan kasir pada bisnis restoran dengan aplikasi POS. *Liputan6*. Retrieved from https://www.liputan6.com/news/read/217790/tips-cegah-kerugian-akibat-kecurangan-kasir-pada-bisnis-restoran-dengan-aplikasi-pos?page=2

Sarker, I. H., Janicke, H., Ferrag, M. A., & Abuadbba, S. (2024). Multi-aspect rule based AI: Methods, taxonomy, challenges and directions. *Internet of Things, 25*, 101110.

Virgeniya, S. C., & Ramaraj, E. (2019). Predictive analytics using rule based classification and hybrid logistic regression (HLR) algorithm for decision making. *International Journal of Scientific & Technology Research, 8*(10), 1509–1513.

Zainuddin, M., Rahman, A., & Sari, D. (2021). Pengaruh teknologi informasi terhadap deteksi fraud di sektor usaha mikro, kecil, dan menengah. *Jurnal Ekonomi dan Bisnis*.

DOI: 10.37531/amar.v5i1.2849

Zhang, C. (2020). Classification rule mining algorithm combining intuitionistic fuzzy rough sets and genetic algorithm. *International Journal of Fuzzy Systems, 22*, 1694–1715.