The International Journal of Digital Accounting Research
Vol. 26, 2026, pp. 81-110
ISSN: 2340-5058

A decision framework for procurement fraud detection: Wisdom from academia and industry

Hanchi Gu. Shanghai University of Finance and Economics, China, guhanchi@mail.shufe.edu.cn

Shaoyu Liu. Indiana University South Bend, USA, sl218@iu.edu

Abstract. Procurement fraud poses significant financial and reputational risks to organizations, yet existing efforts to address it are fragmented between academia and industry. While academic research has proposed sophisticated fraud detection models using machine learning and data analytics, these solutions often lack practical applicability due to limited guidance for practitioners. In this study, we address this gap by proposing a decision framework for procurement fraud detection, synthesizing insights from existing literature and a real-world data analytics project with a global brewing company. We identify three critical decision problems in developing fraud detection models: (1) constructing fraud indicators, (2) determining the aggregation level, and (3) selecting the model validation method. By evaluating alternatives for each decision, we offer practical solutions that organizations can tailor to their unique procurement processes and risk profiles. The proposed framework combines the knowledge from literature and practical insights, offering actionable guidance for practitioners while bridging gaps between academic research and industry practice. This study contributes to the field by formalizing decision-making challenges in procurement fraud detection and fostering collaboration between academia and industry.

Keywords: Procurement; transaction fraud; fraud detection; decision problem.

DOI: 10.4192/1577-8517-v26_3

Submitted May 2025
Accepted April 2026

1. INTRODUCTION

Procurement, the process of acquiring goods and services, is critical to an organization's operations, directly influencing profitability and ethical practices. According to research by McKinsey, procurement accounts for a significant portion of global corporate expenditures, often responsible for up to 70% of a company's total revenue, making even slight cost reductions critical for enhancing profitability and operational efficiency (Marques et al., 2023). To safeguard operations, organizations rely on stringent rules, regulations, and standards. However, non-compliance—whether accidental or deliberate—can lead to irregularities, including fraudulent activities (Akalp, 2023; Andrade et al., 2016). Procurement fraud is not only among the most prevalent forms of corporate crime due to the complexity and high volume of transactions in the procurement process, but also one with the highest potential financial and reputational costs for organizations (Jans et al., 2011; PWC, 2024), which can significantly disrupt organizational operations and erode stakeholder trust. In response, stakeholders increasingly demand firms to continuously improve and optimize their procurement cycles. These efforts aim to enhance operational effectiveness, ensure compliance, and detect or prevent fraudulent procurement transactions.

To identify and prevent fraud in procurement, the general industry practice is implementing internal control policies to oversee the procurement cycle, such as segregation of duties and a three-way match. Industry practice also performs some tests to ensure their procurement transactions comply with their internal control policy. Internal audit functions within an organization can help detect fraud (Coram et al., 2008), primarily by sampling transactions to detect irregularities.

However, the traditional procurement fraud detection method is limited to performing tests on a subsample of the population transaction and providing reasonable compliance assurance. Sampling inevitably raises the concern of leaving out key transactions (No et al., 2019). Since fraudulent activity in the procurement area has the highest financial impact on the organization (Oliverio et al., 2019), any loophole or weakness in the procurement cycle can significantly impact the firm's revenue. Thus, effective fraud risk detection analytics should operate at the level of detailed financial transactions (Bay et al., 2006). However, as the amount of transaction data has grown massively, checking financial transactions for details can no longer be performed manually (Bănărescu, 2015). A computer-assisted

technique is needed to perform transactional-level analysis to detect any potentially fraudulent transactions omitted by manual examination.

Given the nature of procurement transactions, procurement is of a relatively higher risk of fraud mainly for two reasons. First, procurement may involve internal employees that can go undetected for years (Davies, 1995). According to the PwC's Global Economic Crime and Fraud Survey conducted in 2020, approximately 40 percent of procurement fraud is committed by internal employees. Employees can take advantage of internal procedures and find loopholes to act on behalf of their interests. Further, potential collusion between an employee and external parties in the procurement cycle work complicates the process of detecting fraud. The top reported risk factor is the process of selecting a supplier (Moody's, 2023), which involves external parties and the possible collusion between business parties.

Second, procurement fraud not only causes monetary loss but also damages the organization's reputation (Westerski et al., 2021). Once a fraud case in the procurement cycle is revealed to the public, the customers will question the quality of products, and vendors will refuse to participate in bidding that is meant to lose. Procurement transactions have a relatively higher risk. The company should be aware of the important aspects they should focus on fraud detection.

Researchers have built fraud detection models on procurement. Ramamoorti and Curtis (2003) propose some conceptual suggestions on procurement fraud detection to government auditors. Jans et al. (2011) build a detection model on addressing fraud committed by internal parties, which are employees related to the company. Alawadhi and Appelbaum (2013) conduct a case study in a large, multinational manufacturer to show the application of computer assisted audit techniques in the procurement card data. Carlsson et al. (2018) build a model based on clustering techniques and past fraud records. Given sufficient past fraud records, Singh et al. (2019) build another fraud detection model. Baader and Krcmar (2018) apply process mining skills to ERP systems to identify fraudulent transactions. Oliverio et al. (2019) use clustering techniques to reduce the records to be tested by auditors. Velasco et al. (2021) detect risk patterns for a government organization in Brazil. More recently, Westerski et al. (2021) cooperate with a large governmental organization in Singapore to design a scoring system for procurement fraud. Recent studies have begun to incorporate graph- and network-based approaches into procurement fraud detection, highlighting the importance of relational structures

among entities. For example, dos Santos et al. (2025) apply graph analytics with structural metrics (e.g., centrality and closed triangles) to identify collusive bidding rings, while Muñoz-Cancino and Ríos (2025) combine machine learning with social network analysis to detect coordinated supplier–bidder behavior in public procurement. Using longitudinal network models, Waxenecker and Prell (2024) show that tightly connected bidder clusters and concentrated spending significantly increase corruption risk. In a related supply-chain context, Zhu et al. (2025) employ a heterogeneous graph convolutional network to capture inter-firm relationships, demonstrating that shared supplier links can propagate fraud risk and improve detection performance. Collectively, these studies suggest that incorporating network-based features can reveal hidden collusive patterns that are not captured by traditional transaction-level analytics.

Despite the sophisticated fraud detection models proposed, existing literature does not systematically summarize the decision problems in procurement fraud detection and these models often suffer from limited applicability due to data dependencies and variability across organizations, hindering their practical adoption in industry settings. We define decision problems as how decision-makers should choose among the alternatives. These choices often have significant consequences. By identifying decision problems in the procurement fraud detection process, a firm can focus on these problems to optimize the effectiveness of procurement fraud detection based on their business characteristics and risk assessment. Therefore, firms lack a clear framework to facilitate their decision-making on fraud detection in the procurement area. This gap in the academic literature and the practical need for evaluating fraudulent behavior in the procure-to-pay cycle motivate our study. Accordingly, this study answers the following research questions:

Research question 1: What are major decision problems in procurement fraud detection?

Research question 2: What can be a decision model to solve the decision problems?

Based on the existing literature and our cooperation with the data analytic team of a global brewing company, we identify three decision problems on fraud detection in the procurement process, (1) constructing fraud indicators, (2) deciding the aggregation level, and (3) choosing the model validation method. We evaluate possible solutions for each decision problem based on industry practice. Then we

propose a new conceptual decision model for procurement fraud detection with the lessons learned from cooperation with the company.

Although procurement fraud detection models in the existing literature have shown a decent performance in their accuracy, the testing results are always data-dependent. Considering the diversity of ERP systems among different companies, the datasets must vary significantly. A model with a good testing result on a single company's dataset may not perform well on another company's dataset. Consequently, the accuracy of the models from the existing literature is not directly comparable. The main contribution of this paper is to summarize existing literature and identify the common decision problems. We analyze the advantages and disadvantages of alternatives for some alternatives to help future model designers make decisions. This paper is especially beneficial for users of procurement fraud detection in the industry. With this research, they will better understand how the models are built. Instead of simply comparing the accuracy of existing literature, they can choose the most suitable alternatives for their companies to build a procurement fraud detection model.

At the same time, the increasing use of data analytics for continuous monitoring of procurement activities raises important ethical and data privacy concerns. The analysis of detailed transactional data may involve sensitive information related to employees and vendors, creating potential risks associated with excessive monitoring, misclassification, and unintended reputational consequences. In addition, regulatory frameworks such as the General Data Protection Regulation (GDPR) impose constraints on how such data can be collected and processed. Therefore, effective procurement fraud detection systems must balance analytical effectiveness with ethical responsibility and data governance considerations.

The next section of the paper provides the background of the procure-to-pay cycle and identifies decision problems in procurement fraud detection. Section 3 proposes a conceptual decision model through lessons learned from the collaboration with a global brewing company, which addresses each decision problem. Section 4 concludes our study.

2. BACKGROUND AND DECISION PROBLEM IDENTIFICATION

2.1. Procurement to pay (P2P) cycle

Understanding the procurement workflow is essential to identify fraudulent activities in the P2P cycle. The procurement cycle usually starts with a purchase requisition, when the requester's needs are identified and the purchase requirements are evaluated (Novack & Simco, 1991). The next stage is vendor selection. The selection of a supplier is one of the critical phases in the purchasing cycle (Davies, 1995). In this stage, firms typically have three ways to find the most competitive supplier or vendor, depending on the purchase value: asking vendors to bid on sizable monetary value purchases, asking vendors to provide a quote for mid-value purchases, or selecting a vendor directly for a small purchase (Westerski et al., 2021). When the vendor is selected, the procurement cycle can move forward to the issuance of purchase order (PO), which contains the detailed information of the purchase and will be used to contract with the selected vendor.

The next stage in the procurement cycle is goods receiving. The firm can contract with the vendor and receive goods delivered by preparing goods receipt note (GRN). The last stage is invoice and payment. In this stage, the firm will perform a three-way match of PO, GRN, and invoice to ensure the purchased item, purchased quantity, and total price match. Once the invoice is approved, the firm can make payment to the vendor. We confirm the procurement workflow shown in Figure 1 with our partner on the procurement-to-pay cycle employed by the industry and consider other related work on procurement fraud detection to describe the procurement workflow that best fits our research.

2.2. Decision problem identification

Despite the extensive literature on fraud detection, the studies that pay special attention to fraud detection in the procurement process are limited. Literature collection includes several phases. We first search different combinations of keywords related to our topic, such as 'procurement', 'procure-to-pay', and 'fraud detection'. Next, we manually read the articles and select studies based on transaction records. We filter out research on datasets other than transaction records. For instance, (Min & Lin, 2018) detect procurement fraud based on signaling data from phone calls, which is irrelevant to our study. We summarized the most relevant literature in the Table 1.

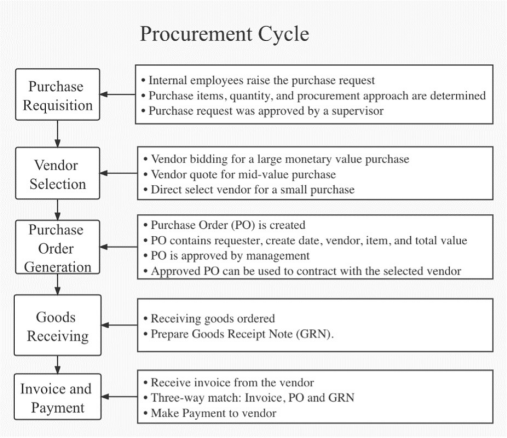

Figure 1. Procurement cycle

Paper	Indicator Description	Indicator Categorization	Aggregation Level	Validation Method
Jans et al., 2011	Not Applicable	Not Applicable	Highly Aggregated Fraud	Industry Experts
Alawadhi & Appelbaum, 2013	Not Applicable	Not Applicable	Highly Aggregated Fraud	The Internal Audit Department
Carlsson et al., 2018	Detailed Description	No Categorization	Highly Aggregated Fraud	Controllers in the Firm
Baader & Krcmar, 2018	Detailed Description	Fraud Type, Stage and Parties Involved	Detailed Types of Fraud	A Simulation
Singh et al., 2019	No Detailed Description	No Categorization	Highly Aggregated Fraud	A Consulting Firm
Oliverio et al., 2019	Detailed Description	No Categorization	Highly Aggregated Fraud	Analysis by Researchers
Westerski et al., 2021	Detailed Description	Procurement Stages	Highly Aggregated Fraud	The Procurement Department
Velasco et al., 2021	Detailed Description	Fraud Type	Detailed Types of Fraud	Public Spending Data from Brazil

Table 1. Existing literature on procurement fraud detection models

We identify three decision problems (1) constructing fraud indicators, (2) deciding the aggregation level, and (3) choosing the model validation method. Any existing or future studies to build models on procurement fraud detection have to make decisions for these three problems. Fraud indicators are the attributes derived from companies' ERP systems, frequently used as input of machine learning models. The aggregation level of fraud determines the result generated from models and are used by the management. The validation measures the reliability for each model. The

designers should be aware of the alternatives to choose from and make the optimal choice.

2.2.1. Decision problems related to fraud indicators – constructing indicators (DP1)

The first decision problem we identified is constructing a list of fraud indicators to detect fraud in the P2P cycle. Existing studies develop models that are built on procurement data in a specific firm. Thus, obstacles exist for other firms to adapt academic research works into their procurement fraud detection processes. (Westerski et al., 2021) cooperate with a large governmental organization in Singapore, identifying 48 fraud indicators. Singh et al. (2019) build the detection model on the real-life purchase process data from a large firm in the telecommunications industry. Instead of using the entire data from the ERP system, Oliverio et al. (2019) select purchase orders from nine countries of different corruption levels. Consequently, there is no proof that indicators in their model can be easily adapted to another firm. On the other hand, Ramamoorti and Curtis (2003) discussed designing tests in a more generalized way. Compliance tests are designed to examine data compliance with certain policies and procedures (Ramamoorti & Curtis, 2003). Pattern tests are used to search for unusual patterns existing in the data (Ramamoorti & Curtis, 2003). To make a wise decision on selecting a detection model, firms should ensure that the variables and indicators from extant studies are applicable to their practices.

2.2.2. Decision problems related to aggregation level – general or specific types of fraud (DP2)

Another critical decision problem is how the firm chooses the aggregation level of fraud in the model. In other words, the firms should determine whether to measure risk based on general fraud types or specific fraud types. The Association of Certified Fraud Examiners (ACFE, 2020) makes a classification of occupational fraud and abuse, shown in Figure 2.

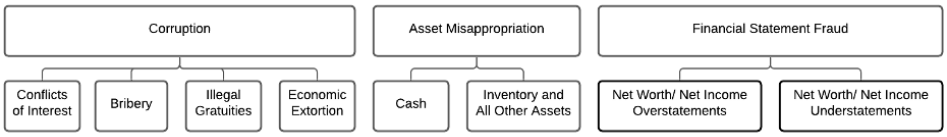

Figure 2. Classification of occupational fraud and abuse (ACFE, 2020)

Corruption, asset misappropriation, and fraudulent statements are three main categories of fraud. Corruption and asset misappropriation are at the transactional level. Corruption includes conflicts of interest, bribery, illegal gratuities, and economic extortion. Asset misappropriation contains two types, the misappropriation of cash and the misappropriation of inventory and all other assets. The risk types can also be further divided into more specific types. For example, ACFE (2020) divides bribery into invoice kickbacks and bid-rigging. Vendors and employees collude to submit inflated or fictitious invoices and share the surplus, which is called kickback (Wells, 2017). There is a bidding rigging if vendors pay to influence the result of competitive bidding (Wells, 2017). Therefore, firms should decide the level of fraud to detect. Naturally, there are lots of methods to divide procurement fraud into different types. In this paper, we define the models' aggregation levels based on the classification of (ACFE, 2020). Therefore, we do not consider models using other classifications such as fraud types based on process mining as models of detailed fraud types.

Some studies are on general fraud types. Carlsson et al. (2018) build a model at a highly aggregated level to label risky transactions. They consider corruption and asset misappropriation together with indicators of mixed fraud types. Singh et al. (2019) apply supervised learning methods to detect fraud transactions without considering any specific kind of fraud. Other researchers assign a score for each transaction at a general level. Oliverio et al. (2019) use simple fraud indicators as red flags and cluster the transactions. For each cluster, they calculate aggregated red flag scores, which cannot directly indicate the fraud type. The transactions in the high-risk cluster need further manual investigation for details. Westerski et al. (2021) build a scoring system for general fraudulent behaviors, but they do not explore a specific risk type listed by ACFE (2020). Therefore, as for the fraud types, they are providing fraud scores at an aggregated level.

While testing highly aggregated levels of fraud are prevalent in the literature, other models consider specific fraud of various types. Baader and Krcmar (2018) map the

fraud indicators to each type of fraud, enabling their model to evaluate fraud types. For instance, they collect 25 indicators for kickbacks. Velasco et al. (2021) use a decision support system, combining operations research tools with advanced data science methods to identify specific types of fraud risks. They successfully highlight collusion, conflict of interest, fake companies, and other types of fraud.

2.2.3 Decision problems related to model validation – choosing the way to test the result (DP3)

Designing a fraud detection model on procurement is the study of providing an effective and efficient way to identify fraud. Model validation is an essential part of an accurate model. In the extant literature, industry experts are assumed to be a reliable source to measure whether the transaction follows the firm's designed procedure (Jans et al., 2011). Controllers in the firm are another source to verify the possible fraud actions. Carlsson et al. (2018) apply clustering techniques to obtain a subset with higher fraud risk, which is sent to the controller for final evaluation. In other studies, real-world validation is difficult to conduct. Therefore, Baader and Krcmar (2018) generate semi-realistic fraud data with a simulation, where participants act as fraudsters. As it is challenging for researchers to achieve reliable fraud validation in the procurement area, they start to collaborate with a specific firm. Singh et al. (2019) closely cooperate with a large firm in the telecommunications industry. A consulting firm was working with this company in the telecommunications industry to conduct forensics auditing for fraud. Similarly, the cooperation between Westerski et al. (2021) and A*STAR facilitates the validation process. The procurement department of A*STAR tests the accuracy of the model.

3. DECISION MODEL: LESSONS LEARNED FROM A PROJECT WITH A REAL-WORLD DATA ANALYTIC TEAM

In this section, we discuss the lessons we learned from the collaboration with the data analytic team of the global brewing company. We propose a conceptual decision model to help a company develop fraud detection models on procurement by addressing each decision problem identified in the previous section. Our proposed decision model is informed in part by a collaboration with the data analytics team of a global brewing company. While this collaboration provides valuable practical insights into real-world procurement fraud detection, it is important to note that these insights are derived from a single organizational setting.

As such, the firm's specific ERP configurations, data structures, and internal control processes may not fully represent those of other organizations, such as small and medium-sized enterprises (SMEs) or public sector entities. Accordingly, the purpose of incorporating industry insights in this study is not to provide statistically generalizable findings, but to inform the development of a conceptual decision framework grounded in practice. Firms adopting this framework should consider their own organizational context, including differences in information systems, data availability, and procurement processes, when applying the proposed decision model.

3.1. Decision model 1: Construct fraud indicators

Since every business has unique practices and policies, we review indicators created by academic research and industry practice to provide relatively more sophisticated and comprehensive indicators set for our audience to choose from. Given the limited number of existing literature on procurement fraud detection, our indicator set is not complete. However, the purpose of this paper is to generalize the indicator construction process rather than to provide an exhaustive list of fraud indicators. Based on the decision model we discuss below, firms can construct their own indicators refer to the list of indicators, adjusting with their business operation and internal risk assessment. We reorganize indicators used by academia and industries based on factors firms can focus on. Firms can refer to Appendix A and Appendix B to find a more detailed description for each indicator then further to obtain a more comprehensive understanding and construct indicators. Firms can construct their procurement fraud indicators based on which factors they would like to focus on in the procurement cycle, either stage of the P2P cycle, parties involved, or transaction variables. Table 2 presents this unified Master Indicator Matrix, where each fraud indicator is characterized along multiple dimensions, including procurement stage, involved parties, and primary transaction variables. This structure reduces redundancy and enables flexible indicator selection based on organizational needs.

Indicator	P2P Stage	Involved Parties	Primary Variable
Shell Companies	Purchase Requisition	Requester, Vendor	Relationship
Share Bank Account	Purchase Requisition	Vendor	Relationship
Common Directors	Purchase Requisition	Requester, Vendor	Relationship
Conflict of Interest	Purchase Requisition	Requester, Vendor	Relationship
Purchase Frequency	Purchase Requisition	Requester	Date
No Request	Purchase Requisition	Requester, Approval Officer	Process
Quick Close (Tender)	Vendor Selection	Requester, Vendor	Date

Fast Evaluation	Vendor Selection	Requester	Date
Closest Winner	Vendor Selection	Vendor	Value
Overpriced Award	Vendor Selection	Requester, Vendor	Value
Award Similarity	Vendor Selection	Requester	Value
Bid Similarity	Vendor Selection	Vendor	Value
Border Value (Tender)	Vendor Selection	Requester	Value
Benford Analysis	Vendor Selection / PO Generation	Vendor	Value
Round Values	Vendor Selection / PO Generation	Vendor	Value
Sensitive Procedure	Vendor Selection	Approval Officer	Process
Sensitive Category	Vendor Selection	Requester	Category
Unusual Vendor	Vendor Selection / PO Generation	Vendor	Relationship
Frequent Invite	Vendor Selection	Requester, Vendor	Frequency
Frequent Award	Vendor Selection	Vendor	Frequency
Single Bid	Vendor Selection	Vendor	Count
Name Patterns	Vendor Selection / PO Generation	Vendor	Pattern
Tender Split	Vendor Selection	Requester	Value
Absurd Estimates	Vendor Selection	Requester	Value
Fabricated Vendor	Vendor Selection	Vendor	Behavior
Late Awarded Bidder	Vendor Selection	Vendor	Pattern
Frequent Loser	Vendor Selection	Vendor	Pattern
Lucky Winner	Vendor Selection	Vendor	Pattern
Unawarded Vendor	Vendor Selection	Vendor	Process
Ghost Vendor	Vendor Selection	Vendor	Status
Virtual Vendor	Vendor Selection	Vendor	Identity
Duplicate Pay	PO Generation	Vendor	Value
Order Split	PO Generation	Requester	Value
Item Spending	PO Generation	Vendor	Value
Vendor Spending	PO Generation	Vendor	Value
Border Value (PO)	PO Generation	Requester	Value
Requester Spending	PO Generation	Requester	Value
Excess Spending	PO Generation	Vendor	Value
Early Approval	PO Generation	Approval Officer	Date
No Approval	PO Generation	Approval Officer	Process
Retrospective PO	PO Generation	Requester	Date
Price Elevate	PO Generation	Vendor	Value
Block/Unblock	PO Generation	Approval Officer	Process
Repeat PO	PO Generation	Requester, Vendor	Pattern
Segregation of Duties (PO)	PO Generation	Approval Officer	Process
Change Vendor	PO Generation	Vendor	Process
Unusual Price	PO Generation	Vendor	Value
Quantity Spike	PO Generation	Requester	Quantity
Late PO	PO Generation	Requester	Date
Mismatch Item	PO Generation	Requester	Process
Goods Not Received	Goods Receiving	Receiving Staff, Vendor	Process
Term Change	Invoice & Payment	Vendor	Process
Unsuccessful Payment	Invoice & Payment	Vendor	Process
Three-Way Match Failure	Invoice & Payment	Vendor	Process
Different Currency	Invoice & Payment	Vendor	Process

Quick Invoice	Invoice & Payment	Vendor	Date
Pattern Invoice	Invoice & Payment	Vendor	Pattern
Different Vendor	Invoice & Payment	Vendor	Process
Segregation of Duties (Payment)	Invoice & Payment	Purchaser	Process
Large Payment	Invoice & Payment	Vendor	Value
Multiple Payment	Invoice & Payment	Vendor	Frequency
Early Payment	Invoice & Payment	Vendor	Date
Increased Payment	Invoice & Payment	Vendor	Value
Purchase from Employee	Invoice & Payment	Vendor, Employee	Relationship
Weekend Transaction	Invoice & Payment	Purchaser	Date

Table 2. Master indicator matrix for procurement fraud detection

3.1.1. Based on stages of P2P cycle

One way is to focus on different stages of the procurement cycle, conducting an internal risk assessment to determine which stage the company wants to put more weight on.

Purchase Requisition. Indicators in the first stage are mainly about requesters making purchases for their own interests and collusion with the vendor. For example, the indicator "Conflict of Interest" is used to detect when a requester makes a purchase request from his personal company (Westerski et al., 2021). Another indicator, "Share Bank Account," is used to recognize different vendors with the same bank account (Oliverio et al., 2019). "No Request" is an indicator used by our partner in the industry practice to detect purchase orders issued without a proper request. Explanations of such industry practice tests can be found in Appendix B.

Vendor Selection. The second is a phase with relatively higher fraud risk as nearly half of the indicators are located in this section. In this phase, major potential fraud risk types include bid-rigging, bid fixing, kickbacks, and advanced fees (Davies, 1995). For example, from the indicators created by Westerski et al. (2021), "Single Bid" can detect bid-rigging by finding a tender that only has one single bidder. "Frequent Invite" can spot specific vendors continuously invited by the requester that indicate potential kickbacks.

PO Generation. In this stage, indicators are developed mainly to identify unusual item prices and unusual PO. For example, the indicator "Price Elevate" stands for purchase price increase after PO creation (Oliverio et al., 2019). The indicator "Item Spending" can find unexpected item price changes by comparing unit prices with average prices from past purchase orders (Westerski et al., 2021). The indicator

"Duplicate Pay" developed by Westerski et al. (2021) is to recognize orders that replicate within the same day. This kind of fraud is also spotted by industry practice. Our partner performed the test "pr_po2" to detect POs that have the same vendor, the buyer (purchasing organization), material group, currency, and amount (without currency conversion), issued less than 30 days after each other (from our Global Brewing Company partner).

Goods Receiving. This stage has a lower risk of fraud because details of the purchase, such as purchase item, item price, and vendor, have been settled in the previous phase, and personnel who actually place the order and receive goods have limited discretion. One indicator here is "Goods not Received", which advises potential theft and asset disapprobation.

Invoice and Payment. The majority of indicators come from industry practice; only limited indicators are used by academic research. "Term Change" and "Unsuccessful Payment" were created by Oliverio et al. (2019) to spot unusual activities in payment. Industry practice primarily focuses on fraud detection in the Invoice and Payment stage. For example, purchase orders without a purchase requisition, invoices without a purchase order, and the invoice date are earlier than the PO date (from our Global Brewing Company partner). Fraud indicators can be constructed based on different phases in the procurement cycle and by considering which parties are involved in procurement fraud.

3.1.2. Based on a combination of parties and P2P stages

Another way is to identify parties involved in fraudulent activities on procurement transactions. A firm can determine which party has a relatively higher risk based on past fraud cases and The Fraud Triangle proposed by Clinard and Cressey (1954). We identified parties involved in fraud cases at each P2P stage by working with our partner and grouped our indicators by parties involved in the procurement fraud scenario.

Purchase Requisition. The major parties involved in the first stage are the requester and vendor. The fraud that happened in the first stage usually appears in the form of the purchase of items without requisition (Singh et al., 2017) or in the form of purchase for the requester's personal interest. For example, "Purchase Frequency" can be used to detect whether the requester's purchase request is within a reasonable frequency range. "Common Director" created by Westerski et al. (2021) can be

used to capture potential collusion between vendor and requester. Suppose the requester makes a purchase request from suppliers that share directors. In that case, it is more likely than not that there is potential collusion between the requester and the common director that needs further investigation. A supervisor responsible for approving purchase requests can also be involved in fraud in the purchase requisition stage. For example, "pr_po5" is a test performed by our partner in their industry practice to capture purchase orders without purchase requests. In this case, an approval officer can generate a purchase order without any requester's original purchase request.

Vendor Selection. The requester and vendor can still collude in the second phase. The requester can pass the information about when the bid will start and stop and the budget limitation to a specific vendor to help the vendor gain insider information and competitive advantage over other vendors. For example, among indicators in the second phase, "Quick Close" and "Fast Evaluation" can detect the time difference between tender notice, tender closing date, and internal evaluation date (Westerski et al., 2021). Management can engage in fraudulent activity in the vendor selection stage by frequently authorizing special procedures, which are usually for particular circumstances. For example, Westerski et al. (2021) created an indicator that the requester frequently uses a limited Invite-To-Quote procedure. Nevertheless, by consulting with our partner, only higher management has the authority to select a particular procedure. We classify the "Sensitive Procedure" into the approval officer group.

PO Generation. In this phase, the requester causes fraud by splitting massive purchases into smaller ones to bypass the limits on a purchase order since a more significant purchase may catch more attention and trigger a stricter purchase procedure. "Order Split" is used by both Westerski et al. (2021) and Oliverio et al. (2019) in their model to capture requesters raising purchase requests in the same day that combines to a huge purchase. Purchasers and vendors are the main parties involved in fraudulent cases in the PO generation phase. Purchasers and vendors conduct collusion on elevating item prices, creating fake purchases with a real vendor. "Item Spending", "Vendor Spending", and "Excess Spending" created by Westerski et al. (2021) can capture the unusual price PO. "Benford Analysis", "Round Value", and "Unusual Vendor" can spot potential fake purchases. Approval Officer involved in fraud cases in the PO generation phase by misuse of one's

approving right. The approval officer can pre-approve a particular PO for a related vendor who sends kickback or bribery to the officer. Alternatively, the approval officer chooses not to approve a legit PO to blackmail the selected vendor.

Goods Receiving. In this stage, receiving specialist is the primary party. Unusual delivery indicates potential theft and embezzlement (Singh et al., 2017).

Invoice and Payment. In the last phase of the procurement cycle, the purchaser is the primary party involved in fraudulent cases. For example, a purchaser conducts small amounts of purchases without formal purchase requests and purchase orders. Based on how different parties are involved in fraud cases in industrial practices, firms can select fraud indicators based on what stage in the procurement cycle and which parties are participating in the purchasing.

3.1.3. Based on purchase variables

A firm can further construct their indicators on the aspects of the purchase they want to detect. The date is one crucial variable. A firm can design the time difference between each step of the procurement cycle. If a later step happens before a former step, there is either a weakness of internal control or fraud. For example, the invoice date should always be later than the PO date. An invoice date earlier than the PO date indicates unauthorize purchases. Quantity is another vital variable. The unusual quantity of items indicates possible embezzlement, inflated quantities to exhaust budget, or accrue vendor kickbacks (Singh et al., 2019). Monetary value is an essential dimension for indicator construction. Unusual item price indicates potential manipulation of costs to fit the budget or siphoning of funds (Singh et al., 2019).

A firm should construct a fraud indicator set that fits best for their operation to detect potential fraudulent activity in the procurement process effectively. Fraud indicators sets can be developed based on stages of the P2P cycle, a combination of stages and parties involved in fraud, or preferred purchase variables.

3.1.4. Network-based indicators

Beyond transaction-based indicators, recent advances in graph and network-based analytics further extend the construction of fraud indicators by incorporating relational structures among entities. Rather than relying solely on transaction-level attributes, these approaches model connections among vendors, employees, and procurement processes to identify patterns such as collusive bidding rings, tightly

connected supplier clusters, or repeated co-bidding behavior. For example, recent work applies social network analysis to procurement data to detect suspicious relationships among suppliers and identify coordinated behavior that is difficult to capture through traditional monitoring approaches (Muñoz-Cancino & Ríos, 2025). Similarly, graph-based machine learning methods leverage relationships among entities to enhance the detection of collusive bidding patterns by incorporating topological features extracted from procurement networks (dos Santos et al., 2025).

Network-based studies further show that structural features such as centrality, clustering, and shared participation in tenders can reveal coordinated behavior that is not observable at the individual transaction level. For instance, prior research demonstrates that collusion and corruption risks are often embedded in network structures such as tightly connected bidder clusters and concentrated contracting relationships (Waxenecker & Prell, 2024). In a related stream of research, supply chain–based graph models show that fraud risks can propagate through inter-firm relationships, highlighting the importance of relational structures in detecting complex fraud patterns (Zhu et al., 2025).

In this context, network-derived features can be viewed as an extension of traditional fraud indicators, enriching the indicator construction process by capturing relational and structural dimensions of procurement activities. Incorporating such features allows organizations to detect more complex forms of fraud, particularly collusion and coordinated manipulation among multiple actors.

3.2. Decision model 2: Decide general or specific fraud detection

The investigation of fraud on procurement is complex, as (ACFE, 2020) provides a detailed classification of fraud and abuse. General anomaly detection on high-level categories such as corruption and asset misappropriation can show the decision-makers aggregated results at a high level. Meanwhile, other models detect more detailed fraud types related to the procurement process, such as conflicts of interest, bribery, illegal gratuities, and fraudulent disbursements. It is clear that procurement fraud is intrinsically a group of diverse types of risks in the procurement process. Decision-making at the aggregation level is important because the models to evaluate all types of fraud at a highly aggregated level are different from models for subdivided fraud.

3.2.1. Based on highly aggregated fraud

The decision-makers can request a model of high-level procurement fraud. This type of model provides an overall estimation for each transaction. One common goal of applying fraud detection models is to downsize the samples, saving the time to evaluate each record. The model built by Carlsson et al. (2018) uses a group of fraud indicators to recognize transactions similar to past fraud records. Although their model lacks explainability, it can successfully identify the abnormal transaction for further investigation. Similarly, Oliverio et al. (2019) calculate the general risk scores for each cluster after clustering transactions based on the fraud indicators. The focus is now the transactions in the riskiest cluster. Time and effort will not be wasted for the low-risk clusters. Correspondingly, the result of such models is a single label or score for each transaction. Decision-makers can easily compare the fraud risks among different vendors or employees and across time periods. However, such models are not free of shortcomings. The results are highly aggregated without details on the sub-categories. Consequently, firms need further manual analyses to understand the results. This type of model lacks the ability to generate explainable results.

3.2.2. Based on detailed types of fraud

A model based on specific fraud types is another option. This type of model measures the risk for various risk types, such as conflicts of interest, fake companies, and kickbacks. The most straightforward advantage of this model is a more explainable result. For each transaction, the model shows which type of fraud it belongs to. In addition, it offers a detailed summary of various non-compliant types, with their amount and frequency. It attracts the firm's attention to educate its employees to avoid the riskiest types of fraud. Nevertheless, there are potential limitations. First, the predefined settings of indicators and risk patterns should be accurate. This type of model relies on the indicators or patterns to recognize various types of risk. If the predefined settings are inaccurate, the value of the model is damaged. Furthermore, as the types of fraudulent transactions are preset, this model cannot identify unexpected fraud types.

This section shows the advantages and disadvantages of general fraud detection or specific fraud detection. A clear fact is that firms can always generate general risk types given a model of detailed types of fraud. Therefore, decision-makers should make trade-offs and select the most suitable aggregation levels for the models based

on their needs. To save time and identify general fraud, the firm can cut off the details sub-categories of fraud and focus on the big picture. On the contrary, a model of explainability should clearly define each fraud type and the corresponding settings of the fraud indicator.

3.3. Decision model 3: Model validation

To evaluate the usefulness of a model, validation of its accuracy is essential. Experts in the industry (Jans et al., 2011), the procurement department in the firms (Westerski et al., 2021), consulting firms (Singh et al., 2019), and simulations (Baader & Krcmar, 2018) are all possible validation methods. As we collaborate with the global brewing company, our team gains insights into two common channels to validate the result. We analyze the strengths and weaknesses of two testing channels, an audit firm as a third party and the firm's procurement department.

3.3.1. Based on third parties

Various third parties can conduct model validation with different procedures. Our analysis focuses on one industrial practice of using a third-party audit firm by our partner. This section introduces how this third-party audit firm tests the transaction for our partner and analyzes the suitable condition for such third parties. The audit firm investigates the public records to identify affiliate parties, which can be vendors in the transactions. More importantly, the audit firm selects transactions and checks important documents from the company, such as purchase requisition, bid process, and contracts with its profession. The advantage is the audit firms' profession. Audit firms are experienced in reviewing documents and identifying risky vendors. They have teams that specialize in this industry, and they can apply the knowledge from other cases to our partner company. One obvious drawback is the extra expense to the audit firm. In addition, this audit firm relies on documents provided to them or publicly available without a field investigation inside the company. Thus, it can neglect some detailed evidence from the company's aspect, such as the department managers' experience and whistleblowers' reports.

3.3.2. Based on the procurement department

An alternative validation method is to cooperate with the procurement department. In industrial practice, an experienced employee can detect fraudulent transactions by manually reading the records. To investigate within the procurement department,

the firm takes advantage of its familiarity with the company. The employees in the procurement department have a better understanding of the department's policies and controls. Therefore, they can find violations of the policies. Furthermore, most firms own some unique knowledge. For example, managers in an overseas branch have more insights into local bribery cases, providing useful information. Despite the advantages, a validation based on the firm itself creates potential risks. Fraudsters within the firm may affect the investigation, lowering the reliability. Additionally, firms lacking a professional internal audit team are not suitable for this method.

In this section, we briefly introduce two possible methods to validate the model. A third-part audit firm evaluates the models professionally with documents and publicly available information. The procurement department of the firm depends more on the employees' experience and unique knowledge. Because of the variety of validation methods, firms have more choices for validation. For instance, a simulation is also an option in the extant literature (Baader & Krcmar, 2018). However, the simulations frequently use students to execute the procurement process. There is no guarantee that their behavior can accurately simulate reality. Therefore, we still prefer a real-world investigation.

3.4. Ethical and data privacy considerations

The increasing use of data analytics and machine learning techniques for continuous monitoring of procurement transactions raises important ethical and data privacy concerns. While such systems enhance the effectiveness of fraud detection, they may also introduce unintended consequences related to employee surveillance, vendor profiling, and the misuse of sensitive information.

First, fraud detection systems often rely on detailed transactional and behavioral data associated with employees and vendors. Continuous monitoring of such data can create perceptions of excessive surveillance, potentially affecting employee morale and trust within the organization. In addition, the use of certain fraud indicators, such as patterns of interactions between employees and vendors or shared personal attributes, may raise concerns regarding fairness and proportionality in monitoring practices.

Second, model-driven fraud detection systems are subject to classification errors. False positives, in particular, may lead to reputational damage for employees or

vendors who are incorrectly flagged as suspicious. Without proper governance mechanisms, such outcomes may result in unintended organizational or legal consequences. Therefore, firms should carefully design escalation and review procedures to ensure that model outputs are interpreted with appropriate human oversight.

Third, regulatory frameworks on data protection, such as the General Data Protection Regulation (GDPR), impose constraints on how personal data can be collected, processed, and used. Organizations operating in jurisdictions subject to such regulations must ensure that their fraud detection systems comply with principles such as data minimization, purpose limitation, and transparency. Similar data protection requirements are increasingly emerging in other regions, further emphasizing the need for compliance-aware system design.

These ethical and privacy considerations are closely related to the decision problems identified in this study. In constructing fraud indicators (DP1), firms should avoid using variables that unnecessarily expose sensitive personal information or that may introduce bias. In selecting validation methods (DP3), firms should incorporate governance mechanisms, such as independent reviews or audit trails, to ensure accountability and fairness in decision-making. Overall, integrating ethical and data privacy considerations into the design of procurement fraud detection systems is essential to ensure that such systems are not only effective but also responsible, compliant, and sustainable in practice.

4. CONCLUSION

This research discusses procurement fraud detection by identifying three decision problems and proposing a decision model to help firms make optimal decisions. Through the literature on the procurement process, we have an understanding of the procurement cycle. Further analyses on literature related to procurement fraud detection help us identify three decision problems. Meanwhile, we cooperate with a global brewing company to have more insights into the industrial practices of fraud detection in the procurement process. Our focus is not to identify specific characteristics of fraud detection in this company but to explore the alternative choices for the decision problems. Industrial practices guide our design of a decision model, which is applicable to all potential users. In addition, the increasing reliance on data analytics for procurement fraud detection raises important ethical and data governance considerations. Continuous monitoring of procurement

activities may involve sensitive information related to employees and vendors, creating potential concerns regarding privacy, fairness, and unintended consequences from misclassification. Moreover, regulatory frameworks such as the General Data Protection Regulation (GDPR) impose constraints on how such data can be collected, processed, and utilized. Therefore, organizations should incorporate ethical safeguards and data governance mechanisms into the design and implementation of fraud detection systems to ensure that these systems are not only effective but also responsible and compliant.

In conclusion, the main contribution of this paper is to facilitate companies to evaluate fraud in their procurement process. The collaboration with our partner company indicates that the procurement fraud detection processes differ among companies because of the variety of parties involved, their information systems, etc. Instead of centering on one firm, our proposed decision model assists firms in solving the decision problems with choices in industrial practices, offering suitable methods to various goals in procurement fraud detection. However, this study still has several limitations. One drawback is that our knowledge of industrial practices is from a single firm. Although our team tries to find complete and universal answers for the decision problems, we may neglect other possible alternatives. Another limitation is that the existing fraud detection literature in the procurement process is limited. The decision problems that we derive from the literature can be incomplete. We expect that there will be more literature published in this area. Then we can have a more complete summary for decision problems.

In addition, emerging technologies such as generative artificial intelligence (GenAI) introduce new challenges for procurement fraud detection. Advances in GenAI may enable the creation of increasingly sophisticated fraudulent artifacts, such as realistic fake invoices, synthetic vendor identities, or manipulated supporting documents. Future research may explore how fraud detection systems can adapt to these evolving threats, for example by integrating document forensics, anomaly detection, and AI-assisted verification mechanisms.

5. REFERENCES

ACFE. *ACFE Report to the Nations: 2020 Global Fraud Study*. (2020). https://legacy.acfe.com/report-to-the-nations/2020/ Accessed 24 June 2022.

Akalp, N. *The Consequences of Noncompliance in Business.* (2023). https://www.corpnet.com/blog/the-consequences-of-noncompliance-in-business/ Accessed 12 February 2025.

Alawadhi, A., & Appelbaum, D. (2013). Expert Knowledge Elicitations in a Procurement Card Environment. *Available at SSRN 2350588*. https://doi.org/10.2139/ssrn.2350588

Andrade, E., van der Aa, H., Leopold, H., Alter, S., & Reijers, H. (2016). Factors leading to business process noncompliance and its positive and negative effects: Empirical insights from a case study. AMCIS 2016 Proceedings.

Baader, G., & Krcmar, H. (2018). Reducing false positives in fraud detection: Combining the red flag approach with process mining. *International Journal of Accounting Information Systems*, *31*, 1-16. https://doi.org/10.1016/j.accinf.2018.03.004

Bănărescu, A. (2015). Detecting and preventing fraud with data analytics. *Procedia economics and finance*, *32*, 1827-1836. https://doi.org/10.1016/s2212-5671(15)01485-9

Bay, S., Kumaraswamy, K., Anderle, M. G., Kumar, R., & Steier, D. M. (2006). Large scale detection of irregularities in accounting data. Sixth International Conference on Data Mining (ICDM'06). https://doi.org/10.1109/icdm.2006.93

Carlsson, C., Heikkilä, M., & Wang, X. (2018). Fuzzy C-Means for Fraud Detection in Large Transaction Data Sets. 2018 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE). https://doi.org/10.1109/fuzz-ieee.2018.8491498

Clinard, M. B., & Cressey, D. R. (1954). Other people's money; a study of the social psychology of embezzlement. *American Sociological Review*, *19*(3), 362. https://doi.org/10.2307/2087778

Coram, P., Ferguson, C., & Moroney, R. (2008). Internal audit, alternative internal audit structures and the level of misappropriation of assets fraud. *Accounting & Finance*, *48*(4), 543-559. https://doi.org/10.2139/ssrn.1021611

Davies, D. (1995). Purchasing and procurement fraud. *Journal of Financial Crime*, *2*(4), 322-330. https://doi.org/10.1108/eb025658

dos Santos, E. S., Castro, M., & Carvalho, J. T. (2025). Improving Public Procurement Collusion Detection With Graph-based Machine Learning Methodologies. Escola Regional de Aprendizado de Máquina e Inteligência

Artificial da Região Sul (ERAMIA-RS). https://doi.org/10.5753/eramiars.2025.16657

Jans, M., Van Der Werf, J. M., Lybaert, N., & Vanhoof, K. (2011). A business process mining application for internal transaction fraud mitigation. *Expert Systems with Applications*, *38*(10), 13351-13359. https://doi.org/10.1016/j.eswa.2011.04.159

Marques, F., Ribeiro, G., & Sjödin, E. *The strategic era of procurement in construction*. (2023). https://www.mckinsey.com/industries/engineering-construction-and-building-materials/our-insights/the-strategic-era-of-procurement-in-construction Accessed 12 February 2025.

Min, X., & Lin, R. (2018). K-means algorithm: fraud detection based on signaling data. 2018 IEEE World congress on services (SERVICES). https://doi.org/10.1109/services.2018.00024

Moody's (2023). *Top 10 supply chain risks that companies face*. https://www.moodys.com/web/en/us/insights/compliance-tprm/the-top-10-supply-chain-risks-that-companies-face.html Accessed 12 February 2025.

Muñoz-Cancino, R., & Ríos, S. A. (2025). Data-Driven Transparency: Machine Learning and Social Network Analysis for Corruption Detection in Public Procurement. *Procedia Computer Science*, *270*, 1788-1795. https://doi.org/10.1016/j.procs.2025.09.299

No, W. G., Lee, K., Huang, F., & Li, Q. (2019). Multidimensional audit data selection (MADS): A framework for using data analytics in the audit data selection process. *Accounting Horizons*, *33*(3), 127-140. https://doi.org/10.2308/acch-52453

Novack, R. A., & Simco, S. W. (1991). The industrial procurement process: A supply chain perspective. *Journal of business logistics*, *12*(1).

Oliverio, W. F. M., Silva, A. B., Rigo, S. J., & da Costa, R. L. B. (2019). A hybrid model for fraud detection on purchase orders. Intelligent Data Engineering and Automated Learning–IDEAL 2019: 20th International Conference, Manchester, UK, November 14–16, 2019, Proceedings, Part I 20. https://doi.org/10.1007/978-3-030-33607-3_13

PWC. *Global Economic Crime Survey 2024*. (2024). https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html Accessed 12 February 2025.

Ramamoorti, S., & Curtis, S. (2003). Procurement fraud & data analytics. *Journal of Government Financial Management*, *52*(4), 16-24.

Singh, N., Cheng, E., & Lai, K. (2017). A Data Analytics–Based Approach to Auditing. *Internal Auditing*, *7*(8), 33-41.

Singh, N., Lai, K. h., Vejvar, M., & Cheng, T. E. (2019). Data-driven auditing: A predictive modeling approach to fraud detection and classification. *Journal of Corporate Accounting & Finance*, *30*(3), 64-82. https://doi.org/10.1002/jcaf.22389

Velasco, R. B., Carpanese, I., Interian, R., Paulo Neto, O. C., & 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

Waxenecker, H., & Prell, C. (2024). Corruption dynamics in public procurement: A longitudinal network analysis of local construction contracts in Guatemala. *Social Networks*, *79*, 154-167. https://doi.org/10.1016/j.socnet.2024.07.001

Wells, J. T. (2017). *Corporate fraud handbook: Prevention and detection*. John Wiley & Sons. https://doi.org/10.1002/9781119351962

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

Zhu, S., Ma, T., Wu, H., Ren, J., He, D., Li, Y., & Ge, R. (2025). Expanding and interpreting financial statement fraud detection using supply chain knowledge graphs. *Journal of Theoretical and Applied Electronic Commerce Research*, *20*(1), 26. https://doi.org/10.3390/jtaer20010026

Appendix A

Fraud indicators

Indicator	Description
Shell Companies	Requester buying from different suppliers, with different directors but both present in some other third supplier
Share Bank Account	A vendor with a bank account used by another vendor
Common Directors	Requester making purchase from 2 different suppliers that share at least 1 director
Conflict of Interest	Requester making purchase from a company where he is also a director
Purchase Frequency	The average difference between purchase dates
Quick Close (Tender)	Time difference between tender notice and closing dates significantly smaller in comparison to typical cycles for past tenders
Fast Evaluation	Time difference between tender closing and final internal evaluation dates suspiciously small in comparison to past tenders
Closest Winner	Winning tender bid and the next closest bid are very close to each other in terms of value
Overpriced Award	Winning bid is not the best cost-wise option in comparison to other bids submitted
Award Similarity	Estimated tender value by requester is very close to actual awarded bid
Bid Similarity	Estimated tender value by requester is very close to submitted bid values
Border Value	Estimated tender value is close to the predefined border (e.g., tender value that involves additional approvals)
Benford Analysis	Estimated tender value is in a subset of purchases with digit frequency deviating from the reference of Benford's law
Round Values	Total awarded value for tender is a round number
Sensitive Procedure	Sensitive tender procedure used to manage tenders of a requester
Sensitive Category	Tender related to purchase of a specific type of goods (possible more prone to fraud than others)
Unusual Vendor	Tender was awarded to a vendor who has little interactions with any other requesters except of one
Frequent Invite	Vendor being frequently invited in tenders by the selected requester

Frequent Award	Vendor being frequently awarded in tenders by the selected requester
Single Bid	Requester participating in tenders that have only a single bidder
Name Patterns	Tender has similar awarded vendor name to other tenders made by the same requester
Tender Split	Tender is involved in a scheme by requester splitting bigger purchases into smaller ones
Absurd Estimates	Proportional to the ratio of APV/EPV
Fabricated Vendor	Requester invites a vendor who is never bidding (i.e., fabricated competitor)
Border Value	EPV is close to the 70k border (tender border)
Award Similarity	EPV is very close to APV value, the closer the more suspicious
Sensitive Procedure	Frequency of use of limited Quote by given requester (the more frequently the more suspicious)
Frequent Spender	Frequency of purchases (the theory is that frequent purchasers could be suspicious)
Quick Close (Quote)	Time difference between Quote notice and closing dates significantly smaller compared to typical cycles for the past Quotes
Fast Approval	Time difference between Quote creation and approval dates suspiciously small compared to the past Quotes
Late Awarded Bidder	Same vendor always coming as the last bidder and winner (collusion with the requester to get other bid data)
Frequent Loser	Supplier frequently not awarded
Lucky Winner	PO with requester–vendor was not awarded but afterward the requester did another EPR and awarded the same vendor
Unawarded Vendor	Different supplier awarded and different supplier for PO
Ghost Vendor	Awarded supplier is not active at the time of award/Sleeping vendor/Supplier marked for deletion/Vendor status in the vendor master is inactive for the vendor listed within open PO
Virtual Vendor	Vendors without address
Duplicate Pay	Order was duplicated multiple times during the same day
Order Split	Order is involved in scheme by requester splitting bigger purchases into smaller ones/PO created by the same person, same vendor, same amount and date/Sequential invoices number from a supplier

Item Spending	Unit prices of items within a PO far from the average for those items as found in past orders
Vendor Spending	PO value differs significantly from the average order value for the particular vendor
Border Value	Order value is close to the limit for untendered order
Round Value	Order value is a round number
Name Patterns	Order has similar vendor name to other orders made by the same requester
Unusual Vendor	Order was made with a vendor that has little interactions with any other requesters except of one
Benford Analysis	Order belongs to a subset of purchases where the value digit frequency deviates from the reference frequency of Benford's law
Requester Spending	PO value differs significantly from the average order value for the particular requester
Excess Spending	PO value greater than APV /Invoice amount higher than the order
Early Approval	PO-approved date is earlier than the EPR-approved date
No Approval	PO performed without approval on the workflow
Retrospective PO	PO created after the invoice date
Price Elevate	Purchase price increase after PO creation
Block/unblock	When a PO is blocked and unblocked
Goods not Received	Goods not delivered for a paid invoice
Term Change	Changes in payment terms for a vendor
Unsuccessful Payment	Payment block

Notes: Fraud indicators synthesized and adapted from Oliverio et al. (2019) and Westerski et al. (2021). PO = purchase order; APV = awarded purchase value; EPV = estimated purchase value, following the terminology in Westerski et al. (2021).

Appendix B

Industrial tests

Feature	Feature Name
Inactive Vendor	Vendor status in the vendor master is inactive for the vendor listed within open PO
Repeat PO	PO have the same vendor, buyer (purchasing organization), material_group, currency and amount (without currency conversion), issued less than 30 days of each other
Segregation of Duties	The same user was responsible for entering and approving the PO.
Change Vendor	Identify vendor IDs that are different between PR and PO
No Request	POs issued without PRs are risky
Unusual Price	POs issued to vendors whose prices seem unusually low or high for material types are risky (40% amount increased)
Quantity Spike	POs issued to same vendor with sudden spikes in the quantities for a material code are risky.
Late PO	POs in which the creation date exceeds the standard period (in 2 working days) are risky (grouped by levels eg: geography, type of vendor, type of PR or material type)
Mismatch Item	Discrepancy/Mismatch in the number of line items and amount between PR and PO are risky POs
Three Way Match	Identification of invoice without a requisition (PR) and with a purchase order (PO)
Different Currency	Different currency between PO and Invoice
Quick Invoice	Invoice date within 5 days of PO date
Pattern Invoice	Invoices with a sequential pattern for the same vendor. Incoming invoices should not have a sequential pattern for the same vendor
Different Vendor	Identify vendors IDs that are different between PO and Invoices
Segregation of Duties	The same person responsible for processing the invoice and releasing the payment
Large Payment	Identify payments to a third party where payments appear for unusual or larger values, i.e., third party normally receives a monthly retainer, and one payment is of a larger amount. (40% increase on the price between the range of 1 year)
Multiple Payment	Multiple invoices paid on the same date and same vendor is a risky transaction

Early Payment	Payments done much earlier than the payment term is a risky transaction (in lesser time when compared to average - 2SD of time taken for payments made to similar vendors for similar materials / services / geography, etc.
Increased Payment	Increase in payments (when compared to the average + 2SD of historic payments made to them if number of historic payments is higher than [x] number of payments) to particular vendors without corresponding increases in goods or services is risky
Purchase from Employee	Payments to a vendor whose address is same as the address of an employee are risky payments
Weekend Transaction	JEs posted on weekends are risky