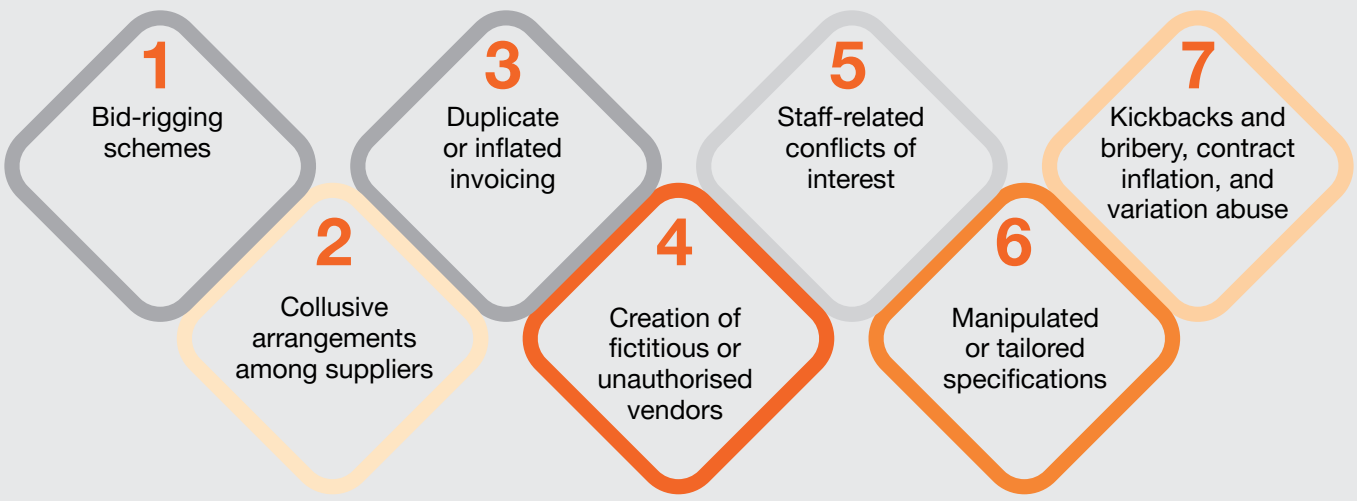
From spend leakage to strategic losses: Procurement fraud risk and its deepening impact on value creation in the Consumer and Industrial Products and Services (CIPS) Industry

Author

Augustina Ekua Mills
Consumer and Industrial Products and Services Leader
augustina.e.mills@pwc.com

Companies operating in the CIPS industry are navigating complex issues including rising supply chain pressures, higher operating costs and shrinking margins which continue to impact performance. At the same time, changing consumer lifestyles are driving a shift in preferences, resulting in more demanding customers who expect tailored and flexible options. Executives are therefore increasingly focusing on redesigning operating models and improving cost structures to digitising supply chains, enhancing forecasting and building more resilient sourcing strategies. Despite the shift in focus, there remains an age-old issue which cannot be relegated to the background. According to the 2024 PwC Global Economic Crime Survey, procurement fraud is one of the three most prevalent economic crimes faced by organisations globally, with cybercrime and corruption being the other two. It is therefore imperative that it remains on the radar of executives and measures should be put in place as companies evolve.

Common procurement fraud schemes include:



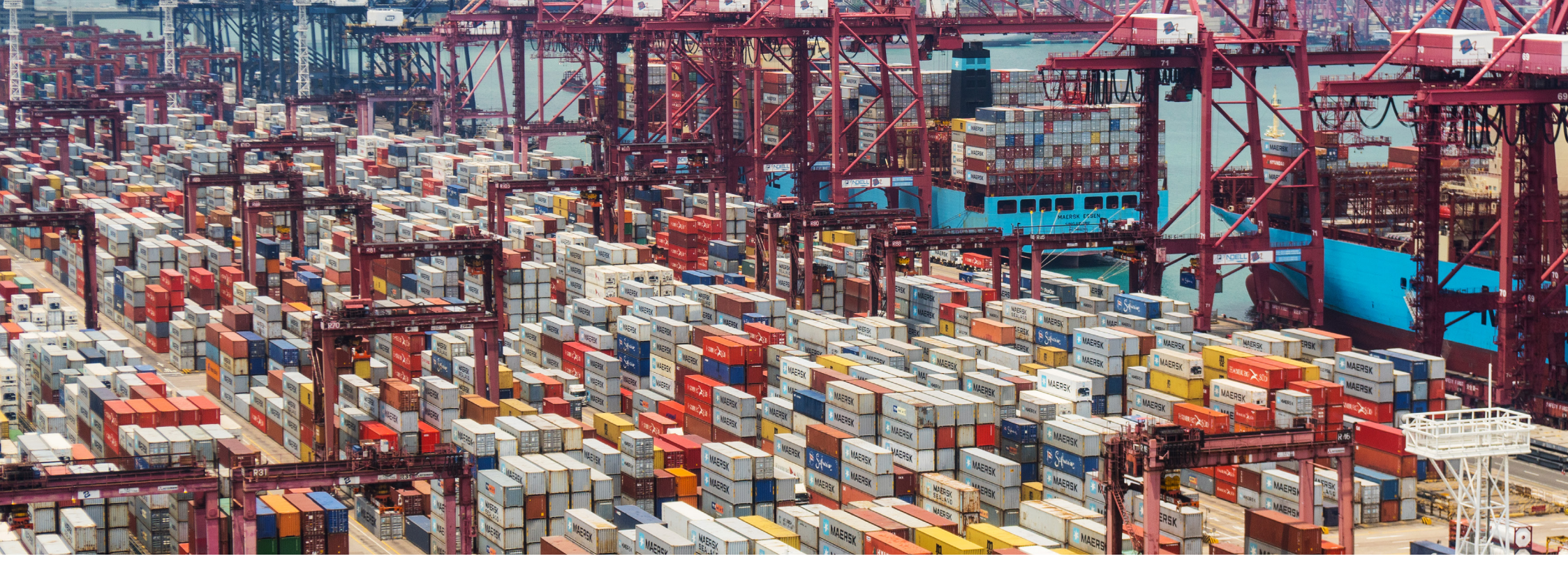
PwC's 2026 AI Predictions anticipated that companies will increasingly adopt higher levels of automation and agentic AI which require minimal human intervention. Until then, false or manipulated data can be inputted into human-fed ERPs for processing. Advanced technology and Enterprise Resource Planning (ERP) systems integrate various functions, support due diligence as part of day-to-day procurement processes and increase efficiency for companies operating within the CIPS space, irrespective of the size or type of the company – small, medium-sized, large, or multinational. However, such systems simultaneously create an opportunity for criminals to perpetrate sophisticated fraud. This is often done under the pretence that the "purchase went through the system" and "the system is working as expected". There may also be instances where unintended or "rogue" automation develops within ERP workflows due to weak automation governance or the excessive use of manual overrides that later become embedded as permanent automated rules. In such cases, unauthorised actions may occur within automated processes, enabling manipulation of key procurement steps - including vendor creation, purchase order approval, and invoice matching - without adequate human oversight. Configuration of approval workflows and control settings in ERPs are therefore crucial to ensure that the potential benefits to be gained from the ERP are maximised.

Modern day sophisticated procurement fraud perpetrated by staff and suppliers include:

- **AI enabled invoice manipulation**: fabrication of invoices and alteration of legitimate invoices.
- **Synthetic vendor creation via identity spoofing**: creation of fake supplier identity.
- **Algorithmic collusion among suppliers**: using AI tools to coordinate prices to gain unfair advantage in bidding.

Implications of procurement fraud

PwC's most recent global survey conducted in 2024 on Economic Crime examined how organisations' experience and respond to fraud. It was revealed that for 55% of C-suite respondents, procurement fraud is a widespread concern in their country, yet only 26% are taking advantage of data analytics to help them to identify irregular trends in procurement. The survey also found that many companies lack awareness of the losses from procurement fraud. About 32% of companies surveyed do not



make efforts to quantify the losses arising from procurement fraud. Another 31% that measure these losses do so on an irregular basis. Due to this, the scale of loss from procurement fraud is not fully identified and tackled.

Procurement fraud has financial implications which include direct financial losses through overpricing, kickbacks and duplicated payments. Within the CIPS industry, instances of these include suppliers inflating prices beyond market value and submitting invoices for duplicate payments. This results in leakages, budget overruns and diversion of funds from other important needs. Overall, companies experience decreased profitability and value which adversely impact stakeholders.

Operational implications, such as disruptions in supply chain and delays in production are also implications of procurement fraud. Procurement fraud typically results in the selection of unqualified vendors who produce substandard products and services. This often disrupts production within the CIPS industry. Companies that are victims of procurement fraud might experience customer dissatisfaction due to substandard goods and services, which then results in lower levels of trust, damaged organisational reputation, and possible fines, penalties or sanctions. Companies may also find themselves entangled in costly legal and non-compliance situations attributable to the low quality of goods and services provided to customers.

Further, the overall strategy of a company is negatively impacted when procurement fraud occurs. Procurement fraud reduces the credibility of information presented to management and board members for their consideration and decision-making. True cost structures are distorted, supplier performance data is inaccurate, and cost drivers are misreported. In instances where reports such as cost saving metrics and supplier selection reports are falsified to appear effective, the procurement strategy may be maintained although it needs to be amended.

Response from leadership

Procurement fraud negatively impacts the potential of a company to create sustained value for stakeholders. Considering the complexity and the constantly evolving environment of procurement fraud, board members and senior management need to take an active role in managing this risk with key considerations mentioned below:

Benchmark procurement policies against industry best practices:

Benchmarking procurement policies against industry leaders or best practices within the CIPS industry allows companies to identify gaps. This also allows for continuous improvement and prevents reliance on outdated standards. Benchmarking also provides insights on current procurement policies to enable senior management to make informed decisions based on insights from industry standards. Indeed, benchmarking gives companies the impetus to streamline workflows, optimise resources, improve productivity and create faster cycle times.

Identify areas where analytics and automation can strengthen controls:

Automation is an important component to introduce into procurement processes because it reduces reliance on manual processes, which are liable to error or manipulation. However, the inclusion of AI agents in complex and high-value workflows will not totally eliminate the risk of procurement fraud. Data analytics can assist with continuous monitoring of procurement data to identify red flags that indicate fraud. Data analytics can also support in identifying duplicate or split invoices, abnormal pricing patterns and the frequent use of single source or emergency procurements. Increasingly, geopolitical supply chain shocks have increased single sourcing risks. Using data analytics tools can strengthen procurement processes by improving visibility over supplier activities, reducing manual intervention, and identifying red flags for quick intervention.

In order to prevent unauthorised actions embedded in automated processes, automated workflow integrity scans can be implemented.

Align senior management and board expectations on the growth–risk relationship to manage procurement fraud:

The rate of growth of a company as part of measures to achieve strategic objectives, creates exposures to fraud risk which must be appropriately managed. Examples of such instances of growth particularly in the case of manufacturing companies include expansion of supplier and distributor networks, accelerated onboarding of vendors, and increased delegation of procurement authority. During accelerated growth, controls may weaken, and opportunities for procurement fraud including inflated pricing, conflicts of interest and vendor collusion may increase. The tone and posture of senior management and board must be clear.

Emphasis should be laid on adherence to procurement control measures, reinforce zero tolerance for fraudulent behaviour, and underscore ethical decision making throughout procurement functions.

Establish and maintain a robust Conflict of Interest (COI) policy:

A robust COI policy is an important governance tool for identifying and mitigating procurement fraud. Procurement activities include managing relationships at different levels and applying discretion in supplier selection, especially within the CIPS industry. This leads to the creation of real and perceived conflicts. A robust COI policy creates a framework for evaluating tenders, ensuring transparency and maintaining integrity throughout the procurement process. This strengthens governance, builds trust and creates the required systems for efficient monitoring.

Reorganise functional silos that undermine effective compliance and risk mitigation:

Criminals undertake procurement fraud by exploiting gaps in communication, accountability and oversight between departments. Fraud can remain hidden for long periods when key departments operate in isolation. Key departments such as finance, legal, compliance and procurement need to collaborate across various levels and increase information sharing and visibility especially within the CIPS industry. This will enable early detection of triggers of procurement risk for the required actions to be taken.

Red flags to watch out for

- Frequent use of emergency procurement or single-sourcing procedures
- Suppliers sharing identical or overlapping contact information
- Employees participating in both vendor selection and invoice approval processes
- Price deviations that cannot be justified by market conditions
- Purchases repeatedly structured just below approval thresholds
- Manual overrides or interventions within ERP workflows

Call to action

As procurement fraud leads to excessive spending and leakages which erode margins and decrease value to stakeholders, leaders in the CIPS industry can no longer afford a reactive stance. Now is the moment to strengthen procurement controls, modernise risk management frameworks, and embed transparency across every layer of the value chain. The shift from spend leakage to strategic losses is real and accelerating.

Take action today—reassess your procurement governance, invest in data-driven fraud detection capabilities, and empower your teams with the tools and insights needed to protect value creation.

Companies should also target the following control areas:

- **Governance**: Introduce COI registers and vendor review committees.
- **People**: Conduct background checks, enforce mandatory leave and ensure segregation of duties.
- **Process**: Have strong Procure-to-Pay (P2P) controls, do three-way matching and ensure vendor rotation.
- **Technology**: Adopt analytics and automation and improve workflow controls.

How can PwC support you

Our team of fraud and risk specialists support businesses to strengthen controls, enhance transparency, and protect value across operations. We deliver end-to-end solutions across the following areas:

- **Fraud, integrity and supply chain risk management**: Targeted fraud risk assessments, discreet investigations, workflow automation, and enhanced supply chain transparency through vendor due diligence, third-party risk management, and contract compliance reviews.
- **Operational and production controls**: Assessment of inventory shrinkage, production-process integrity, and asset-protection measures across warehouses, plants, and logistics operations.
- **Financial and commercial risk management**: Revenue-assurance and margin-protection reviews, working-capital optimisation, and independent financial and operational assessments.
- **Regulatory compliance**: Design and enhancement of compliance programmes and risk reviews.
- **Digital, data and analytics solutions**: Digital forensics and eDiscovery, and process mining to uncover anomalies and strengthen decision-making.

Contributor

Esther Addei
Manager, Deals
esther.a.addei@pwc.com

© 2026 PwC Ghana. All rights reserved. PwC Ghana refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see **www.pwc.com/structure** for further details.