



Anti-Fraud Technologies in Procurement: How Data and Automation Are Closing Longstanding Gaps

Due to limited resources, it is not possible for every organisation to produce everything independently. Resource constraints have therefore compelled organisations at the national, regional and global levels to work together to fulfil one another's needs. This may involve the supply of raw materials, high-tech equipment and machinery, as well as services such as construction and consultancy. Procurement is the process of identifying needs, searching for suppliers or vendors, and negotiating the prices and costs of goods or services. While definitions may vary slightly across sources, an effective procurement process generally incorporates a number of core operational steps.

For any organisation, procurement represents one of the areas through which substantial amounts of money can leave the organisation without immediate visibility. Audit professionals frequently identify procurement as a high-risk area, not necessarily because procurement personnel are dishonest, but because the process contains numerous discretionary points at which decisions can be manipulated without detection for extended periods. Procurement fraud occurs when an individual deliberately manipulates sourcing, tendering, contracting or payment processes to obtain financial or other benefits dishonestly. The critical distinction between an error and procurement fraud is intent: fraud involves knowingly circumventing established rules or controls for an improper purpose.

How Procurement Fraud Happens

Procurement fraud generally occurs through several recurring patterns, with bid rigging among the most common. In bid rigging, competing vendors collude in advance to determine who will win a tender. Participants may take turns submitting losing bids so that the group can maintain artificially high prices while preserving the appearance of competition.

Another common form is kickbacks and bribery. In such cases, an official directs a contract towards a favoured vendor in exchange for a personal benefit. Such benefits may be disguised as consulting fees, employment opportunities or arrangements involving relatives or associates.

A third form involves fictitious vendors. Under this scheme, an organisation is invoiced for goods or services that were never supplied or performed. Shell

companies established for such purposes may, upon investigation, be linked to an employee's address, bank account or other personal interests.

Other forms of procurement fraud include invoice fraud and overbilling, undisclosed conflicts of interest, splitting purchases into smaller transactions to circumvent approval

thresholds, and change-order abuse. In the latter case, a supplier may submit a low winning bid and subsequently increase the contract value through variations or additional work that was not subject to the original competitive process. In practice, procurement fraud schemes may involve a combination of two or more of these methods operating simultaneously.



Muhammad Nawaz
MS Scholar in Commerce
Allama Iqbal Open University

The Seven Common Types of Procurement Fraud



Figure 1: The seven fraud patterns that recur most often across procurement audits worldwide.

Why Procurement Fraud Continues to Occur

The recurrence of these fraud patterns across countries and industries can be understood through the well-established concept of the fraud triangle: opportunity, pressure and rationalisation. Individuals may rationalise fraudulent behaviour by convincing themselves that such conduct is acceptable because others are doing the same.

The risk becomes more significant in procurement when individuals have control over substantial financial resources and considerable decision-making authority.

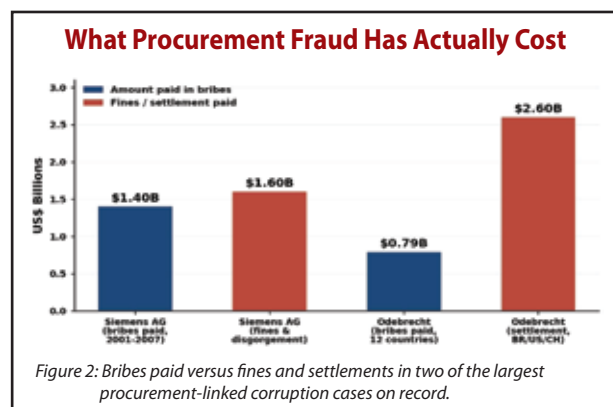
In developing economies, reliance on manual processes can further increase the opportunity for fraud. Physical files can be altered, removed or destroyed, while fragmented records may make it difficult to establish a complete audit trail.

What Traditional Controls Missed

For decades, the primary tools for preventing and detecting procurement fraud were largely manual and periodic. These included segregation of duties, post-transaction internal audits, policy checks, reference checks and supplier blacklists. Such controls remain valuable and have successfully identified numerous cases of procurement fraud. However, their effectiveness is limited by their reliance on sampling and periodic review.

Sampling can detect only those transactions selected for examination. A fraudulent scheme spread across hundreds or thousands of transactions may continue for years without appearing in a sampled transaction. Furthermore, when controls are applied primarily during an annual audit, the funds may already have been transferred and the supporting documentation may have been altered or organised to conceal the underlying activity.

The financial consequences of undetected procurement-related corruption can be substantial. Between 2001 and 2007, Siemens paid more than \$1.4 billion in bribes to secure contracts ranging from national identification systems in Argentina to metro lines in Venezuela. Following its settlement with US and German authorities in December 2008, Siemens paid approximately \$1.6 billion in fines and disgorgement, making it one of the largest Foreign Corrupt Practices Act sanctions on record.



Similarly, Brazilian construction company Odebrecht was involved in corruption across multiple countries and ultimately paid substantial penalties and settlements. The Petrobras “Car Wash” scandal also resulted in significant financial losses associated with overpriced contracts. These cases demonstrate how procurement fraud and corruption can become deeply embedded in business operations when fraudulent practices remain undetected for extended periods.

What Technology Is Doing Differently

One of the most significant changes in modern procurement is the shift towards continuous transaction monitoring. Instead of reviewing a sample of transactions periodically, automated systems can assess transactions as they occur and identify potentially unusual activity. For example, a system can flag duplicate payments as soon as they are recorded.

Artificial intelligence and machine learning can take this capability further by identifying deviations from normal purchasing patterns across vendors, categories and transactions. The systems can identify behaviours such as a vendor repeatedly submitting bids that are just high enough to lose while remaining part of a recurring bidding pattern, or purchases being deliberately divided to remain below approval thresholds.

Benford’s Law can also be used as an analytical technique to identify unusual distributions of leading digits in financial data. When combined with modern anomaly-detection techniques and machine-learning models, such methods can provide an additional layer of analysis for identifying invoice batches or financial records that may warrant further investigation.

Strengthening Vendor Master Data

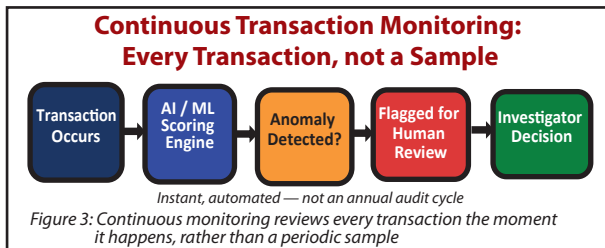
Vendor master data is another important area where technology can strengthen procurement controls. Automated systems can continuously screen vendors against relevant watchlists and other control databases. Changes to vendor bank details can be subjected to dual approval, while system-based access controls can restrict who is authorised to create or modify vendor records and payment information.

Blockchain and Record Integrity

Blockchain technology addresses procurement risks in a different way. Once a record is entered into a properly designed shared ledger, it becomes significantly more difficult to alter it retrospectively without detection. Such controls can reduce opportunities for fraudulent backdating or unauthorised modification of procurement records.

Connecting Data Across Systems

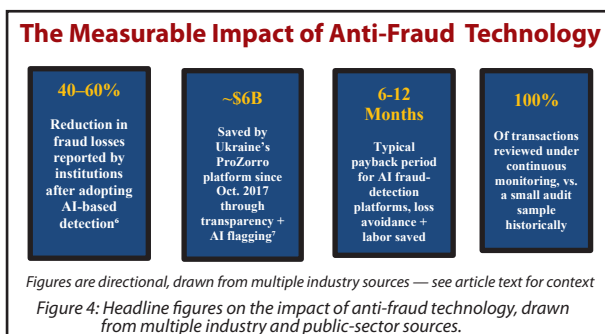
Fraud schemes can also exploit gaps between different organisational systems rather than weaknesses within a single system. Cross-system AI can therefore provide additional value by correlating information from email, enterprise resource planning (ERP) systems and



payment platforms. This can help identify patterns that may remain invisible when each system is analysed separately.

The Impact of Anti-Fraud Technologies

According to Feedzai/Orbograph industry survey data, close to 40% of financial institutions that had adopted AI-based fraud detection reported reductions in losses of between 40% and 60%. Ukraine's ProZorro procurement system, which combines transparency mechanisms, blockchain-based record-keeping and AI-supported flagging, has been credited with generating substantial savings. Similarly, India's Comptroller and Auditor General (CAG) announced in 2026 that it was using AI tools and advanced data analytics to scan public tenders, identify pricing



anomalies and detect potential bid rigging. These developments indicate that advanced analytical tools are increasingly being incorporated into public-sector audit and procurement oversight.

The initial cost of technology can be higher than that of traditional manual controls. Manual controls may largely be incorporated into existing staff responsibilities, whereas automated systems require investment in software licences, ERP integration, data cleansing and implementation. However, once automated systems are operational, the marginal cost

of analysing each additional transaction can fall substantially.

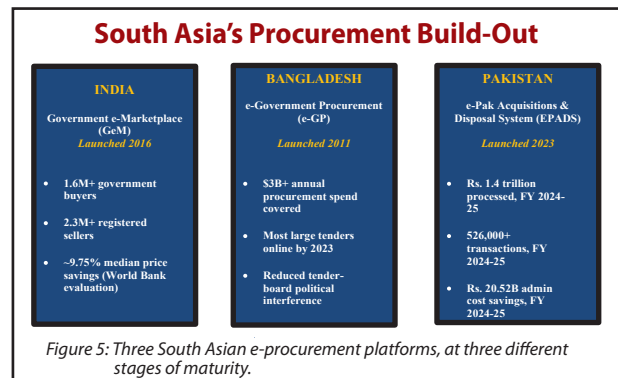
In some cases, organisations may achieve a return on investment within six to twelve months when avoided losses and staff time savings are considered. However, successful implementation depends heavily on proper integration and configuration. Poorly tuned AI systems operating on inaccurate or incomplete vendor data can generate excessive false alerts and may ultimately cost more than the losses they prevent.

Why Technology Matters More in Developing Economies

The case for adopting anti-fraud technology becomes particularly compelling in developing economies where audit capacity may be limited relative to procurement volumes.

South Asia provides several examples of digital procurement at different stages of development. India's Government e-Marketplace (GeM), launched in 2016, represents a relatively mature example. According to the available data, it connects more than 1.6 million buyers with over 2.3 million sellers. An independent World Bank evaluation found that buyers achieved median price savings of approximately 9.75%. At the same time, India's CAG has highlighted the need for stronger benchmarking of GeM's savings methodology, demonstrating that digitisation alone does not automatically guarantee effective oversight.

Bangladesh's e-GP system has been operational since 2011 and had moved most large tenders online by 2023. Pakistan has also expanded digital procurement through the Public Procurement Regulatory Authority's Electronic Procurement System (EPADS). During FY2024–25, EPADS reportedly processed 526,239 transactions worth Rs. 1.408 trillion and generated administrative cost savings of Rs. 20.52 billion. The system has also been connected with institutions including FBR, NADRA, SECP and PEC, with oversight access for bodies such as the Auditor General, NAB and the Competition Commission.



For countries where internal audit teams are consistently outnumbered by procurement volumes, automated tools are increasingly becoming a necessity rather than simply a modernisation initiative. Technology can expand the coverage of audit and monitoring functions without requiring organisations to increase their audit workforce proportionately.

The Future of Anti-Fraud Procurement

Despite the potential of these technologies, their adoption should not be interpreted as an argument for replacing human judgment with algorithms. Presenting technology in such terms would overlook important limitations associated with automated decision-making.

Research and practice concerning trustworthy AI in public procurement continue to highlight the importance of effective governance. If an AI model is deployed without appropriate oversight, it may incorrectly flag a legitimate supplier as suspicious without providing a sufficiently transparent basis for the decision. Such an outcome can cause significant harm to businesses and undermine confidence in the procurement process.

An AI-based system should therefore be sufficiently explainable for auditors and procurement professionals to understand why a particular transaction or supplier has been flagged. The responsibility of accountants and auditors to exercise professional scepticism does not disappear simply because an algorithm makes the initial assessment. Instead, their role expands to include reviewing the model, its thresholds, the quality of its underlying data and the processes through which flagged suppliers or transactions are investigated.

Procurement fraud often thrives on transactions that appear routine, insignificant or anonymous and therefore receive limited scrutiny. Continuous monitoring and pattern detection are steadily reducing the opportunity for such activity to remain hidden. However, organisations that derive the greatest value from these technologies are unlikely to be those that simply invest in the most sophisticated platforms. Rather, the strongest results come from organisations that combine technology with capable professionals who are willing to challenge anomalies and ask the fundamental question that has always been central to good auditing: Why should I believe this?

Conclusion

The transformation of procurement through data and automation represents a significant shift from periodic detection towards continuous prevention. Traditional

controls such as segregation of duties, audits and supplier checks remain important, but technology can extend their reach by analysing transactions at scale, identifying unusual patterns and connecting information across multiple systems.

The objective is not to eliminate human involvement from procurement oversight but to enable professionals to focus their expertise where it matters most. AI, machine learning, continuous monitoring, blockchain and stronger vendor-data controls can provide earlier warnings and broader visibility, while accountants, auditors and procurement professionals remain responsible for interpreting those signals and taking appropriate action.

Ultimately, anti-fraud technology is most effective when it is supported by reliable data, sound governance and professional judgment. The real opportunity is therefore not simply to automate existing controls, but to create a procurement environment in which unusual behaviour is identified earlier, investigated more effectively and becomes increasingly difficult to conceal.

References

- Association of Certified Fraud Examiners, Report to the Nations — the fraud triangle framework of opportunity, pressure, and rationalisation is a long-standing staple of fraud examination literature.
- U.S. Securities and Exchange Commission, "SEC Charges Siemens AG for Engaging in Worldwide Bribery," press release 2008-294, December 15, 2008. sec.gov/news/press/2008/2008-294.htm
- U.S. Department of Justice, "Siemens AG and Three Subsidiaries Plead Guilty to Foreign Corrupt Practices Act Violations," press release, December 15, 2008. justice.gov/opa/pr/2008/December/08-crm-1105.html
- Harvard Law School Forum on Corporate Governance, "2016 Year-End FCPA Update," January 19, 2017 (Odebrecht/Braskem settlement detail); Willkie Compliance Concourse, "Odebrecht Monitorship Comes to a Close," November 2020 (final \$2.6 billion penalty).
- Mongabay, "Brazil's Lava Jato Investigation: The Biggest Corruption Scandal of the Last Decade," March 2025; Petrobras Form 20-F filings, U.S. Securities and Exchange Commission (sec.gov/cgi-bin/browse-edgar).
- AllAboutAI, "AI Fraud Detection Statistics 2026," citing Feedzai/Orbograph industry survey data. allaboutai.com/resources/ai-statistics/ai-fraud-detection
- Harvard Kennedy School, Mossavar-Rahmani Center for Business and Government, "Overcoming Corruption and War: Lessons from Ukraine's ProZorro," 2022; U.S. Strategy on Countering Corruption, December 2021. hks.harvard.edu/centers/mrcbg
- World Bank, "How Government e-Marketplace Is Revolutionizing Procurement in India," World Bank Blogs; Press Information Bureau, Government of India, GeM assessment note, 2022. blogs.worldbank.org/en/governance
- Public Procurement Regulatory Authority (PPRA), Pakistan, official announcements on EPADS FY 2024–25 performance and administrative savings. ppra.gov.pk/announcements

About the Author: Muhammad Nawaz is an MS Scholar in Commerce at Allama Iqbal Open University (AIOU) and is currently engaged in MS thesis research. In addition to academic pursuits, the author serves as a permanent government employee with the Federal Board of Revenue (FBR). He is also a freelance researcher with research interests spanning business, economics, public governance, public policy, taxation, and accountancy.