Introduction to “Integrity Filters”

Automated fraud detection systems for eProcurement and ERP systems

IACRC.org
What are “Integrity Filters”? 

Integrity Filters are sophisticated algorithms to detect and prevent fraud or irregularities that can be embedded in eProcurement and IFMIS Systems.

The Filters can run proactively, to identify possible fraud or before bids are evaluated or payments are approved, or ex-post, against procurement data stored in historic databases.

Algorithms include automated background checks of firms and individuals.
Benefits of eProcurement

According to the *Copenhagen Consensus*, eProcurement yielded a “fantastic’ $663 in benefits over traditional paper procurement systems for every dollar invested in Bangladesh.

THE ECONOMIST, MAY 7, 2016
The Benefits of Integrity Filters

Integrity Filters can analyze masses of documents, such as those from an actual case, below, virtually instantly, compared to the weeks that may be necessary for a manual review.

Integrity Filters exploit electronic procurement data to:

- Block non-compliant transactions
- Provide instant *proactive* alerts of possible fraud
- Instantly review 100% of all transactions
- Permit real time remote monitoring by donors or oversight agencies
- Create detailed audit trails and digital evidence for investigators
- Identify evidence of previous or on-going misconduct in historic databases
Types and levels of reports

**Significant procurement statistics**
e.g., number of contracts awarded to certain contractors by certain approving officials

**Economy and efficiency indicators**
Selection of best product for best price, receipt of discounts or rebates, etc.

**Compliance reports**
Contracts in violation of procurement rules, e.g., Short notice, bids from debarred company, sole source contracts > sole source limit, etc.

"SPQQD" reports
Selection, Price, Quantity, Quality and Delivery indicators that can point to fraud or abuse

**Fraud, waste and abuse reports**
Collusive bidding and bid rigging; False and inflated invoices, shell company vendors etc.
Some common fraud and corruption schemes that can be detected by Integrity Filters

- Collusive bidding
- Bid rigging
- Kickbacks
- Conflicts of interest
- False, inflated and duplicate invoices
- Shell companies
- Phantom vendors
- Purchases for personal use or resale
Sample integrity filters to detect or prevent Tendering Frauds
Color-coded Lists of Indicators

RED: Real-time BLOCKS or ALERTS of significant indicators, e.g., warning of a bid submitted by a debarred company or different bids from the same IP address

BROWN: Pre-programmed REPORTS for other common procurement fraud schemes, waste or abuse

ORANGE: Other less common reports to be listed in a HANDBOOK or ONLINE GUIDE for auditors, investigators or other users

BLUE: links to online public record, telephone and address information
Bid Rigging

Improper manipulation of the bidding or vendor selection process to favor certain suppliers and exclude others

Sample indicators include:

- Procurement official’s contact info = bidder’s info
- Shorter notice to submit bids than the rules require
- Sole source awards > sole source limits
- Recommended award to debarred bidder
- Multiple purchases just < procurement threshold
- Split purchases to avoid competitive bidding
- Award to only one evaluated bidder
- Award to other than the low bidder
- Unusually high or low line item bids in winning bid + change order extending or dropping line item
- Low bid award followed by change order increasing price
- Winning bid price = cost estimate
- “SPQDD” analysis (Selection, Price, Quantity, Quality and Delivery Indicators); e.g.,
  - high #, % of awards to one bidder
  - bid prices significantly > norm
  - quantities significantly > norm
- High # of change orders vs. the norm

Primary data sources:
bidder contact info
- Bid notice and due date
- Procurement rule, e.g. competitive bid thresholds
- Winning and losing bids
- Debarment list

Other potential data sources:
- Line item bid prices
- Contract date and price
- Change orders and amounts
- Previous similar tender results
- Procurement plan info
Collusive Bidding

Secret agreements by bidders or suppliers to divide work and artificially inflate prices, often with the complicity of government officials

Sample indicators include:
• Bids from the same IP address
• Bidders with same contact info
• Bids with same content, errors, etc.
• Unusual bid patterns, e.g., bids an exact % apart
• Sequential bid securities
• Bidders bid in same order in later rounds
• Losing bidder becomes subcontractor
• High price bids; e.g. bids that exceed cost estimate by > 30%
• Pattern of rotation of winning bidders
• Same bidders always bid, win and lose
• Bid patterns differ from prior patterns
• Losing bidders can’t be located in corp. directories or on the internet

Primary data sources:
• Bidder’s contact info, IP address
• Winning and losing bids
• Bid securities
• Cost estimates
• Subcontracts

Other data sources:
• Bids in prior similar tenders
COLLUSIVE BIDDING CASE

Indicators:
- 1 percentage point steps variance from ABC
- Bid price difference: the designated winner ascends in 10 mio CU steps
- Strange and unnatural final bid price numbers

Evidence:
- Companies B, C and F are disqualified
- Severely overpriced earthworks component

Cost Estimate:
104(1)d Embankment
191,930 m³ at 265.17 (unit price) = 50,894,239.32

© INT, The World Bank Group
Reproduction and further distribution requires INT's prior consent
Sample Graphic Reports of Collusive Bidding Indicators

Blue and orange highlighted bids indicate potential collusion.
Sample integrity filters to detect or prevent Purchasing Frauds
False, Inflated and Duplicate Invoices

Sample indicators include:

False invoices:
• Invoice info does not match PO, receiving or payment info
• Sequential invoice numbers
• Broken sequence invoice numbers
• Outliers in price and quantity
• Benford’s Law violations
• Missing info on PO, invoice or receiving doc

Inflated invoices:
• Invoice price, quantities > PO price, etc.

Duplicate invoices:
• Invoices with same #, dates, quantities, item description or amounts
• Total payments > total invoice amounts

Primary data sources:
• PO, invoice, receiving and payment info:
  o Dates
  o Invoice numbers
  o Item #, description
  o Price and quantities
  o Receiving info
  o Payment amount

Other data sources:
• Procurement plan info
• Benford’s Law distributions
"Shell Company" Vendors

Vendors secretly owned or controlled by procurement personnel

Sample indicators include:

- Vendor located at a non-business address or not listed on the internet
- HR/vendor matches (cell phone #s, etc.)
- Vendor not on Approved Vendor List
- Multiple direct purchases > sole source threshold
- Multiple purchases just < competitive thresholds
- Split purchases
- Segregation of duties (SoD) violations
- SPQDD factors
- Vendor provides variety of disparate goods or services vs. norm (per vendor codes and product codes)
- Prompt payment vs. the norm

Primary data sources:

- Vendor master file
- HR master file
- PO, receiving, invoice, payment info
- Procurement rules; thresholds
- SoD requirements

Other potential data sources:

- Benchmark prices
- Vendor and product code lists
Phantom Vendors

Sample indicators include:
- Vendor not listed in corporate registries, directories or on the internet
- Vendor located at non-business address
- Paid vendor not on Approved Vendor List
- HR/Vendor match
- “Fuzzy match” vendors with different bank accounts
- High # or % of sequential invoice numbers
- Broken sequence invoice numbers
- Purchases just < competitive thresholds
- Split purchases
- Small initial purchase
- Payment to inactive vendor account
- One time vendor payment
- Benford’s Law violations
- Vendor provides hard to verify goods, works or services (per product code)
- Incomplete PO, invoice or receiving info

Primary data sources:
- Approved and paid vendor lists
- HR and vendor master files
- PO, invoice, receiving, payment info

Other potential data sources:
- Procurement rules, thresholds
- Benford’s Law distributions
- Vendor and product code lists
Purchases for personal use, resale or diversion

Sample indicators include:
- Purchase of inappropriate personal “consumer items” (per vendor or product codes)
- Different “ship to” address
- Purchased items not in inventory
- Returns without vendor credits
- High # of purchases of items susceptible to personal use (laptops, tires, gas, etc.)
- Split purchases
- Multiple purchases just < thresholds
- Small initial purchase
- Incomplete info on PO or invoice
- Purchased items, volumes differ from procurement plan
- Employee has outside business (used to resell or divert products)

Primary data sources:
- Vendor and product codes
- Purchased item vendor & product codes
- PO, invoice, shipping and receiving records
- Procurement rules, thresholds

Other potential sources:
- Returns and credits
- Inventory records
- Procurement plan info
Benford’s Law

“Law of the first digit” used in fraud detection

In naturally generated numbers, the number 1 is the first digit 30.4% of the time, with other numbers appearing as the first digit in descending order (as in the graph below left)

Prices in invoices, quantities in reports, etc. that do not follow this pattern can indicate fabricated numbers and fraud

\[ P_D = \frac{\int_{\log_{10}2}^{\log_{10}3} P(x) \, dx}{\int_{\log_{10}1}^{\log_{10}10} P(x) \, dx} = \log_{10} \left( 1 + \frac{1}{D} \right) \]
Integrity Filters

Methods to Limit “False Positives”
The primary risk in electronic fraud detection

Identify unambiguous indicators
Such as PO info does not match Invoice; duplicate invoices; different bids from the same IP address

Identify and prioritize other strong indicators
Such as bids from different bidders that are an exact % apart; sequential bid securities

Identify patterns and repeat transactions
Such as high number of % or split purchases by the same procurement official from the same supplier

Identify transactions with multiple indicators
Such as high number of red flags associated with a single purchase or procurement official

Link indicators to reports of fraud
Look for indicators to confirm or rebut a whistleblower complaint or audit concern
Scoring of Fraud Risks

Fraud Risk Levels

Based on detected indicators

Example:

**HIGH RISK**
80-100 points
70% chance of fraud

**MODERATE RISK**
60-79 points
50% chance of fraud

**LOW RISK**
20-59 points
20% chance of fraud

BASE % OF RISK ON PRIOR RESULTS

Example:

Potential Scheme: Change Order Abuse

Indicators:

1. Sole source contract award price just below competitive threshold:
   - One time = 4 points
   - Two times = 6 points
   - Three times = 8 points

2. Followed by change order increasing price to above competitive threshold within:
   - 30 days = 10 points
   - 60 days = 6 points
   - 90 days = 3 points

Fraud Risk Levels

Based on detected indicators

Example:

**HIGH RISK**
80-100 points
70% chance of fraud

**MODERATE RISK**
60-79 points
50% chance of fraud

**LOW RISK**
20-59 points
20% chance of fraud

BASE % OF RISK ON PRIOR RESULTS
Steps of proof with Integrity Filters

1. Apply Filters to eProcurement files to identify suspect transactions, e.g., unusual bid patterns
2. Conduct online and other background checks of the suspect firms and individuals
3. Complete the necessary follow up steps to resolve the issues; see, e.g., https://guide.iacrc.org/proof-of-common-schemes/