ROMANIA

Reimbursable Advisory Services Agreement on

Support to the Implementation of the Public Procurement Strategy (P158629)

OUTPUT 8

Report on the Support for the Supervision Function

January 2020

MINISTERUL FINANȚELOR PUBLICE
AGENȚIA NAȚIONALĂ PENTRU ACHIZIȚII PUBLICE

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

Disclaimer

This document is a product of the International Bank for Reconstruction and Development / the World Bank. The findings, interpretation, and conclusions expressed in this paper do not necessarily reflect the views of the Executive Directors of the World Bank or the governments they represent. The World Bank does not guarantee the accuracy of the data included in this work.

This document does not necessarily represent the position of the European Union or the Romanian Government.

This report has been delivered under the Reimbursable Advisory Services Agreement on *Support to the Implementation of the Public Procurement Strategy* signed between the National Agency for Public Procurement and the International Bank for Reconstruction and Development on September 1st, 2016, as amended. It corresponds to Output 8, under Component B "*Re-engineering the recipient's functional set up and work flows to enable better policy formulation, dissemination, implementation, performance measurement and further policy refinement"*, Activity 3 "***Providing support to ANAP for the development of its supervision function which should ensure the transparency and efficiency of the public procurement system by creating a proactive mechanism for identifying system dysfunctions, including their nature and origin, and performing corrective actions in cooperation with other relevant authorities****",* of the above-mentioned agreement.

Table of Contents

List of Abbreviations

ANAP	National Agency for Public Procurement
BRIAS	Bid Rigging Indicator Analysis System
CA	Contracting authority
CNSC	National Council for Solving Complaints
COMCO	Swiss Competition Agency
CPV	Common Procurement Vocabulary
EU	European Union
ERP	Enterprise Resource Planning
GDP	Gross domestic product
HR	Human Resources
IFMIS	Integrated Financial Management Information Systems
IP	Internet Protocol
LKPP	Indonesian National Procurement Agency
MET	Monitoring European Tenders
OECD	Organization for Economic Co-operation and Development
PDF	Portable Document Format
PEP	Politically exposed persons
PP	Public Procurement
RAS	Reimbursable advisory services
SICAP	Public Procurement Electronic System
SKU	Stock Keeping Unit
SPQQD	Selection, Price, Quantity, Quality and Delivery
UK	United Kingdom
US	United States
WB	World Bank

1. Background

1. The National Public Procurement (PP) Strategy adopted in 2015 foresees the development of the supervision function which should ensure the systematic observation of the public procurement system both at national level and at the level of contracting authorities/entities.
2. The supervision unit was established within ANAP in order to ensure the adequate administrative capacity for the processing of the data and for initiating measures meant to correct the deficiencies in the public procurement system and to ensure its transparency and efficiency. ANAP Order no. 1760 was adopted in 2019 with the purpose to establish how ANAP will interact with the contracting authorities/entities with regard to the supervision activity on how the procurement system is functioning.
3. The supervision activity is based on the data provided as a result of exercising the functions of monitoring, ex-ante control, conciliation, as well as the information received from other sources, as it is considered necessary during the performance of the supervision activities. The supervision activity results in proposal for systemic measures that need to be taken in order to improve the performance of the system and of the contracting authorities/entities, if the case. These can include proposals for instructions and/or guidance, modifications of the PP legislation, or notification of the relevant authorities, such as Competition Council or control bodies, in case of irregular behavior.
4. Thematic actions are developed by the supervision team with the aim to identify the necessary measures to be adopted in order to streamline procurement processes at system level. A first thematic action has already been conducted based on the analytics report provided by the monitoring unit with regard to reasons for cancellation of public procedures.
5. The PP Strategy also envisages the development of a proactive mechanism for the identification of system dysfunctions including their nature and sources and for making corrective actions in cooperation with other relevant competent authorities. The World Bank (WB) team is providing advisory services to help ANAP implement selected priority measures envisaged in the Public Procurement Strategy and meet ex-ante conditionalities in the public procurement area. In this context, the WB was requested to provide expertise for the identification of relevant red flag indicators, including information on programs to detect red flags of potential irregularities in procurements supervised by ANAP.
6. The Reimbursable Advisory Services was amended on August 22, 2019 to include a new activity for *providing support to ANAP for the development of its supervision function which should ensure the transparency and efficiency of the public procurement system by creating a proactive mechanism for identifying system dysfunctions, including their nature and origin, and performing corrective actions in cooperation with other relevant authorities. This activity includes:*

    - *assisting ANAP develop a framework of red flag indicators and related methodology for spotting irregularities both at the national level and at the level of contracting authorities;*
    - *assisting ANAP to develop methodologies for data analysis, problem identification and initiation of corrective actions based on available historical procurement and contract data; and*

- *training nominated ANAP staff on the methodologies and instruments developed above.*

2. Introduction

7. This report discusses:

    - The recommended methodology to install and operate a red flag indicator system: the basic steps to effectively detect, interpret and follow up on red flag indicators as the SICAP system is currently configured;
    - The indicators that can be run in the current SICAP system;
    - The indicators that can be run against additional data if it becomes available in the future. The most useful of such additional data would be:
        - invoice and payment information
        - line item detail in bids and receiving documents
    - The methodology and indicators that could be run if a proactive (ex-ante) detection system is installed in SICAP in the future.

8. The Legal Agreement refers to "creating a proactive [emphasis added] mechanism for identifying system dysfunctions" and "methodologies for data analysis, problem identification and… corrective actions." However, even if a lot of data is available, the current SICAP system is not configured to run a "proactive mechanism" (i.e. that would flag potential irregularities in real time) and does not contain sufficient data to run the full array of red flag indicator tests for "problem identification."

9. The system can be modified, by the e-procurement administrator in coordination with ANAP, to run proactive tests and include the missing data, which consists primarily of invoice and payment information and line item detail in bids and receiving reports, as discussed below. In the meantime, the system can be accessed to produce ex-post reports, also as discussed below.

3. Methodology for data analysis, problem identification and corrective action

10. It appears that much of the SICAP system data is uploaded from PDF documents or electronic submissions and stored in an underlying database that is used to populate the SICAP functions and screens.

11. The typical methodology to look for indicators in such systems would be to:

    a. Determine the indicators (also referred to as "tests") to be run on an ex-post basis. These typically would include indicators:

        - To test controls;
        - To test compliance requirements;
        - In response to complaints;
        - In response to concerns identified in previous or current supervision activities or audits;
        - Suggested by the results of risk assessments or other circumstances.

    b. Ensure that the necessary data to run the selected indicators is in the system or can be imported.

    c. "Clean" and format the data as necessary. For example, correct misspellings, typos and inconsistences (e.g. same street address listed as "st," "Str." "Street," etc.).

    d. Choose the appropriate software, which could be a commercial, off the shelf package, a modified version of the commercial product or an internally developed solution. This is primarily an IT-driven decision to ensure compatibility between the SICAP system design and software.

    e. Write the code – algorithms - to access the underlying database(s) and to identify the desired indicators. The algorithms, once written, can be run repeatedly or modified as necessary.

    f. It should be remembered that in most cases the indicators are merely pointers to possible misconduct – symptoms of potential irregularities or fraud – and not conclusive evidence of wrongdoing.

    g. Run the tests against the data.

    h. Conduct the tests in a manner that reduces the number of "false positives" as much as possible.

       Dealing with "false positives" - red flags of potential irregularities that have an innocent explanation - is one of the primary difficulties in implementing a digital fraud detection program. False positives are particularly disruptive if the fraud detection algorithms are too general or are not tailored to the risk environment being examined.

       False positives can be reduced by the following measures:

        - Identify unambiguous indicators, such as bids from ineligible bidders;
        - Identify and prioritize other strong indicators, such as in bids from different bidders that are identical or an exact percent apart;

- Identify repeat transactions and patterns, such as multiple red flags linked to the same supplier and procurement official, and
- Identify transactions with multiple indicators, such as a high number of red flags associated with a single purchase.

Another important factor in reducing false positives is to link the indicator tests to complaints or specific concerns of potential misconduct. In such cases the indicators are used to confirm or rebut the prior complaints or concerns, rather than to detect possible problems ab initio. This use of the indicators often produces the most useful results.

i. If a red flag is detected:
   - If the red flag suggests an isolated error or irregularity, take steps to correct or address the issue as required;
   - If the red flag suggests a serious irregularity or potential fraud, look for other indicators of the suspected misconduct. Patterns or multiple indicators are more significant than a single indicator.

   For example, if the test reveals unreasonably short notice in a request for bids, indicating possible bid rigging under the EU Directives, look for other indicators of bid rigging, such as:
   - Fewer bidders than the norm; or
   - The award of a competitive contract to a single bidder;
   - An unusually high percentage of previous contract awards to the winning bidder, by the same Contracting Authority;
   - Complaints by other bidders.

j. When electronic indicator detection steps are exhausted, manually collect and examine additional information that may be necessary to resolve the issues, such as, in the above example, the adequacy of information in the bid notice or the reasons for the few bidders. This may include interviews of relevant personnel that has relevant information or was part of the process under discussion.

k. Consider the use of a scoring system to evaluate and prioritize the significance of the detected indicators and related information.

l. Attempt to eliminate legitimate explanations.

   For example, bids submitted by different bidders from the same IP address may reflect the common use of a server or public internet access sites by small, rural firms.

m. If it appears that the issues raised by the indicators and related information suggest possible fraud, refer the matter to the appropriate authorities. Make sure the referral contains all available information of interest to the authority in a well-organized format.

n. Recommend and implement remedial measures, as appropriate, and monitor to ensure compliance.

3.1. Indicators that can be run against currently available data in the SICAP system

12. Below are sample indicators that can be run against the purchasing and tender data currently collected by the SICAP system, in the absence of line item detail in bids and receiving documents and invoice and payment information. It is recommended that ANAP establishes or re-confirms with the administrators of the eProcurement system the conditions for receiving access to the information uploaded by the tenderers at the end of the procurement process as well as the level of availability of data in a format which can be processed by ANAP, in accordance with the in-house practices. The internal procedures should specify the roles and responsibilities in relation to collection and analysis of data from SICAP.

Selection Irregularities

Indicator	Data availability within SICAP
Different bidders with same address or contact info (e.g., address, telephone number, including mobile phones, fax and email address, company contact personnel)	Yes
Unusual bid patterns, e.g. • Identical bids submitted by different bidders, or bids from different bidders that are an exact percentage apart • Winning bids that are much higher than estimated prices or previous bid prices	Yes, but requires receiving access to the documentation uploaded in the system and processing of data related to: Financial offer Estimated budget Financial offers in other similar tenders
Rotation of winning bidders by location, time, product type, etc. This is an indicator which could be subject to the activity of the supervision unit in view of their current attributions. This indicator can be assessed at country level or sector level in order to identify any eventual irregular pattern.	Yes, requires processing of data related to: Bids submitted by the same tenderer Bidders offering same category of products
The same bidders always bid together and the same bidders always win and lose This is an indicator which could be subject to the activity of the supervision unit in view of their current attributions. This indicator can be assessed at country level or sector level in order to identify any eventual irregular pattern	Yes, requires processing of data related to consortia and result of the evaluation process

Indicator	Data availability within SICAP
Short notice to prepare bids This is an indicator which could be subject to the activity of the supervision unit in view of their current attributions. This indicator can be assessed at country level or sector level in order to identify any eventual irregular pattern	Yes
An unusually high number of contracts to the same economic operator by the same Contracting Authority (CA) vs. the norm (i.e., a statistically significant "outlier" in the number of contracts awarded to one firm) This is an indicator which could be subject to the activity of the supervision unit in view of their current attributions. This indicator can be assessed at country level or sector level in order to identify any eventual irregular pattern	Yes
A statistically unusually high percentage of contract awards to the same economic operator by the same CA (v. the number of bids submitted; e.g. one economic operator wins 9 out of 10 proposals) This is an indicator which could be subject to the activity of the supervision unit in view of their current attributions. This indicator can be assessed at country level or sector level in order to identify any eventual irregular pattern	Yes

Unexplained High Prices (such an analysis would require access to the financial offers available within SICAP)

Indicator	Data availability within SICAP
Much higher price for an item than the estimated price, prior prices, catalog prices or prices paid in a similar region for the same item, etc. By item it is understood each component that forms the total price (for example, in a works contract, items are the individually priced materials). Therefore, price and price increases usually refer to an individual, specific item, which is often identified by a unique "SKU" number.	Yes, however within the financial offers submitted by the bidders as well as previous contracts. Access to individual offers and contracts as well as the collection and processing of data is needed.

Indicator	Data availability within SICAP
Higher priced item selected over lower priced offers prices.	Yes, however this may require access to individual offers. Development of the eProcurement system to allow recording unit prices could be envisaged.
Very high % price increases for the same item by the same supplier within the reporting period v. the norm ("outlier" calculation). This refers to a price increase by a vendor for a particular item, such as "X brand copier paper," (or a particular line item in a works contract), that exceeds the average price increase for identical products sold by other vendors by a significant amount during the relevant time period. For example, supplier A increased the price of X brand copier paper during the previous fiscal year by 50% when other suppliers of the same product increased their prices by an average of only 5%. The 50% price increase was an "outlier" because it was the highest such price increase (or a statistically significant price increase) for the Brand X copier paper during that time period. This indicator refers to prices accepted and paid by the purchaser.	Same as previous.

High Quantity Purchases

Indicator	Data availability within SICAP
Very high quantity purchases of an item (v. procurement plans, prior purchases, purchases for the same or similar items in similar regions, etc.) This is an indicator which could be subject to the activity of the supervision unit in view of their current attributions. This indicator can be assessed at country level or sector level in order to identify any eventual irregular pattern.	Yes, for regular items / products (such as paper, fuel etc.) purchased in different regions
Very high % increases in purchase volumes of an item v. the norm (outlier)	Yes, same as previous

Indicator	Data availability within SICAP
This is an indicator which could be subject to the activity of the supervision unit in view of their current attributions. This indicator can be assessed at country level or sector level in order to identify any eventual irregular pattern.	
Unnecessarily high-volume purchases of certain items v. economic need, inventory levels, etc.	Yes, data on purchases is available within SICAP, however the opportunity of the purchase is an issue which would need assessment on a case by case basis.

Low Quality Purchases

- Economic operators with the highest number or percentage of cancelled contracts, rejections or returns. The calculation of this indicator requires access to contract implementation data. By cancelled contracts it is understood the termination of contract after its signature due to fault of the economic operators. Rejections and returns refer to non-acceptance of delivered items, performed services or works due to justified reasons and which are accordingly documented during the contract implementation.
  Considering that the indicators of low quality are not available in the current system, it would be useful if future versions of SICAP could capture this data because of the obvious importance of identifying poor quality goods and services provided by certain vendors.

Other

- The purchase of items suitable for personal use, identified by vendor or CPV code or item description
  Such schemes involve company or government employees improperly charging to their employer the purchase of items intended for their own personal, non- business use.

  Identifying such purchases by vendor code:

  - It is a common fraud by company or government personnel to purchase goods for their personal use, such as consumer electronics, household supplies, or personal apparel, and charging it to their employer, describing the goods as other items suitable for business use. This fraud can be detected by identifying the vendor code of the supplier, which would show it sells items for personal use, not the business items as claimed.

    For example, in an actual case, executives of an oil company purchased expensive items for household improvements and charged them to their employer as "factory parts." The supplier had a general name which did not identify it as a household supplier, but its vendor code did identify it as such.

  Identifying purchases for personal use by product code:

  - Purchases for personal use also can be identified by product codes that identify the type of product or service supplied. Typical examples again include household

items, consumer electronics and apparel purchases. This detection method is most often used to identify personal purchases made through the use of purchasing cards - credit cards issued by the employer to the employee intended to be used only for business purchases.

"CPV code" refers to product code. Comprehensive lists of vendor and product codes can be imported and run against your transactions.

3.2. Red flag indicators that could be detected with additional data

13. As noted above, the most important of **useful additional data** are:

- Invoicing and payment data;
- Detailed, line item bidding data;
- Detailed, line item receiving information.

14. Invoice, detailed receiving and payment information can be used to detect the following schemes and irregularities:

- False inflated duplicate invoices
  - Invoice amount > contract value;
  - Invoice items or quantities don't match receiving records or contract terms;
  - Invoice and payment records don't include entitled discounts;
  - Payment amount > contract value or invoice amount;
  - Payment of duplicate invoices.
- Ghost supplier
  - Sequential invoice numbers (i.e., a high percentage of invoices from a supplier for a six-month period are sequential; e.g., 101, 102, 103, or numbers that fall within a narrow range; e.g. 101 – 110);

  - Broken sequence invoice numbers. This indicator is found when two or more suppliers with the same or very similar names have different invoice numbering systems; e.g. one supplier's system uses three numerical digits: "404," the other's uses four digits and an alphabetical letter: "1234B." This can indicate that one of the suppliers is a ghost using the name of a legitimate supplier.
    Some ghost suppliers try to copy the name of a legitimate supplier exactly or as close as possible to help avoid detection. In some such cases the ghost is careless and inadvertently chooses a different invoice numbering system than the legitimate supplier, as described above, revealing that it is a separate entity, and with further investigation, a ghost.
    Different invoice numbering systems for what purport to be the same vendor was identified as one of the leading indicators of ghost suppliers by an experienced forensic auditor employed by a very large US company.

  - Small initial purchase: the initial total purchase amount from a particular vendor is less than 25% (adjustable + or -) of the average subsequent purchase amount.

    In some cases, the operator of a new fictious company is afraid of detection and decides to "test the waters" by first submitting an invoice in a small amount, hoping that that it will be too small to attract attention. If the invoice is approved, the operator gains confidence and thereafter submits larger and larger invoices.
    This algorithm is designed to detect such behavior by identifying the above trend in which the average amount of subsequent invoices is a certain, adjustable % higher than the amount of the original invoice.
    Invoice as used here refers to approved and paid invoices.

  - Purchases, invoices or receiving documents dated on a weekend or holiday

15. Additional tests can be run as additional data is collected or imported. For example, the **following data could help identify ghost suppliers**:

- Business directory information (the absence of listings in such directories could indicate a ghost supplier;

- List of high-risk addresses (e.g., mail receiving services):
  Some organizations routinely compare their vendor addresses against imported lists of "high risk addresses" to identify ghost suppliers. Here "high risk" means a high risk of fraud associated with such addresses, the most common example in the US being the addresses of mail receiving services, which simply rent mail boxes but which often are presented by ghost suppliers as legitimate business addresses.

- Benford's Law applications;

  Benford's Law[1] states that in naturally occurring number sets, the number 1 will occur as the first digit about 30.4% of the time, the number 2 about 17% of the time with the other digits descending in regular order until the number 9 that appears as the first digit about 4% of the time. Prices in invoices, quantities in reports, etc. that do not follow this pattern can indicate fabricated numbers and fraud.

- PEP or company watchlists or ineligible entities:
  PEP refers to "politically exposed persons," which can be identified from imported lists provided by compliance companies. The purpose of the lists is to identify officials that could be involved in potentially corrupt transactions.
  "Company watchlists or lists of ineligible entities" refers to lists of companies that have been debarred (declared ineligible for future contracts because of their involvement in fraud or corruption) by international organizations, such as the WB, or government entities.
  All of the above lists can be imported and run against the names of vendors or persons doing business thru SICAP.

The attachments provide for additional examples of useful indicators and data requirements.

[1] https://en.wikipedia.org/wiki/Benford%27s_law

3.3. Modifications to SICAP to facilitate the collection of relevant data and detection of red flags

16. The most important modifications to SICAP that would facilitate the automated, proactive analysis of procurement data would be to:

    - Provide a standardized, structured bid submission form on the SICAP website to be employed by all SICAP bidders and vendors. This form would contain pre-identified fields that would be populated by the bidders or suppliers, down to line item detail. Obtaining the data in this structured format would greatly facilitate the ex-ante identification of indicators.
    - The fields should include that information necessary for the broadest feasible application of the red flag indicators without unduly burdening the procurement process.
    - The data requirements and indicators contained in the SICAP system should be tailored to the needs of SICAP and ANAP, *by identifying the indicators and related data requirements of schemes **as they occur in Romania***, rather than merely installing generic indicators or indicators run in other systems. For example, the indicators of cartel activity and collusive bidding often differ depending on the country where the collusion takes place, and may be different in Romania than elsewhere.
    - Sophisticated text reading and pattern recognition Artificial Intelligence programs could be added to review bid notices, bids, contracts and invoices and identify red flags. Much more detail on these programs is available on request.

      "Sophisticated text reading programs" refers to computer programs that can read and analyze information in text documents (and not just numbers, as in standard data analytics programs). See, for example, the UK program discussed below, that has the ability to identify similar text and word count in different bids. Such similarities in the wording in bids is the number one red flag of collusive bidding.

      "Pattern recognition Artificial Intelligence programs" refers to computer programs that can themselves identify previously unknown patterns and indicators of fraud in data, without the indicators being previously input into the program by a human operator. See, for example, the Swiss COMCO case example at p. 28, below, in which the Swiss Competition Agency (COMCO) was able to detect previously unknown indicators of collusion in bids in a particular canton n Switzerland.

17. Considering that the administration of the e-Procurement system lies with a different institution, ANAP may initiate discussions at Government level if it considers that any of the above recommendations meets the objectives of the PP strategy and may facilitate the work of the supervision team. Finally, it should be remembered that automated detection systems are no panacea, and that such measures should be integrate with other standard supervision and detection procedures.

4. Workshop

On December 17, 2019, a World Bank team working on the RAS delivered the workshop on "Red flags indicators". The audience comprised ANAP members of the supervision unit, but also monitoring and public policy units (participants are mentioned in annex 3).

During this session, the WB experts carried out a presentation of the proposed red flags indicators and methodology as well as of the application that illustrates the results based on fictive data.

The audience provided feedback during the workshop which was focused mainly on:

- The role of the supervision unit which is not related to fraud identification but on identification of irregular behaviors that influence the public procurement system;
- The need to identify system-level indicators to complement the list of indicators which are more applicable at agency level, in line with the provisions of the PP Strategy. This could be a 2-layer mechanism for identification of irregularities, at system and agency level;
- The proposed indicators should reflect what can be done with the available data;
- The need for a plan for the development of the supervision function which should highlight what is currently available, what should be further improved and where there is need for interinstitutional or interdepartmental cooperation;
- Roles of monitoring and supervision units related to data collection and analysis should be clarified in terms of what is to be provided by monitoring unit and what should be further developed by the supervision staff;
- The report should present the scoring for the indicators.

The WB team explained that the proposed list of red flags indicators reflects the provisions of the legal agreement and that further development of the supervision function could be envisaged within the assessment of the PP system and related action plan.

On the scoring aspect, the team appreciates that there is no general risk scoring criteria for indicators; many agencies or audit groups that use red flag indicators do not use any scoring system at all; and for those that do, the scores are assigned by the agency that use the indicators. The list of indicators from the currently available data are all significant indicators, meaning that any one of them they should attract the attention of procurement personnel and auditors and require explanation. A number or pattern of indicators listed there, such as the improper selection of a vendor followed by the payment to it of unreasonably high prices, or the purchase from it of unnecessary large quantities, or both, would of course be more significant than a single indicator.

As an example of how indicators might be prioritized, APPENDIX A to the Supervision Report is edited to include color codes indicators to show their significance; **red** being the most significant indicator and **brown** a less significant indicator, but still important. A short paragraph on risk scoring is included under point 5 of Annex 2.

The edited version of APPENDIX A, referred to above, include indicators that require data that is not currently available in SICAP. This is to illustrate how the additional data - including invoice and payment information and line item receiving information - greatly improves the effectiveness of the red flags system. The collection of this additional data also would make it easier to assign risk scores to the indicators and to match them to the related schemes.

A list of system-level indicators foreseen by Chapter 5 of the PP Strategy which could be used as basis for further analysis in view of identification of irregular behaviors by the supervision unit is attached as annex 4.

Recommendations

In order to better focus the activity of the supervision unit considering its role according to the PP Strategy as well as the need to complement the activity of other main institutions responsible in the area of fraud, corruption and audit, ANAP should consider implementing working procedures and related capacity development programmes that could include:

- Review of the existing working procedures related to data analysis and better clarification of roles of monitoring and supervision units;
- Training of staff in data science and data analysis in order to acquire the needed skills such as programming skills in Stata and R (potentially in Python). Such courses are offered by universities or could be accessed online. The implementation of the training plan may run in parallel with attracting staff with such skills either as employees or as part of internship programmes run by the Government. Development of a training plan in this regard would help the agency further improve the supervision function and allocate the corresponding budget accordingly.
- Workshops in identification of irregular patters in public procurement based on public procurement data, including data interpretation, should be also considered. This could include aspects such as the use of the red flags system, how to interpret and prioritize the indicators and the follow up steps.
- Interinstitutional mechanisms – the development of the supervision function in order to allow for the implementation of all the indicators proposed in the present report might require the modification of the legal framework and putting in place cooperation agreements or protocols to ensure the availability of the relevant data and the coordination of activities. A proper analysis of the current situation – both legal and institutional – could be envisaged under a separate assignment. Section 3.1 of the report identifies what could be currently done and for which we recommend ANAP to take initiative and start the dialogue with the relevant authorities – in particular, the administrator of the eProcurement system and CNSC – in order to better determine the framework of the cooperation.

5. Annexes

Annex 1 Prioritized Red Flag Indicators List

Annex 2 Red Flag Indicators: Explanation and the International Experience

CONTENTS

1. Introduction to red flag indicators – what they are and their benefits

Red Flag Indicators (hereinafter "indicators") are algorithms to detect indicators of fraud, waste, abuse, errors and irregularities in electronic procurement data. Many of the algorithms are based on proven forensic accounting tests that have been used for decades; others were developed more recently as the result of lessons learned in procurement fraud audits and investigations.

The algorithms are particularly effective when installed in eProcurement, Enterprise Resource Management (ERP) or Integrated Financial Management Information Systems (IFMIS), such as SAP, Oracle and FreeBalance. This is because many such systems offer easy, real-time access to the masses of well-organized data that they collect and store, without the burden of manually collecting and converting paper records to electronic files.

The indicators can be run on a continuous monitoring basis, with ex-ante real time alerts of potential fraud, or on an ex-post basis. The indicators also can be run against databases of historic procurement data to identify red flags of previous fraudulent practices, such as on-going cartel activity.

The indicators installed in procurement systems can be an important component of an overall eGovernment program because most serious fraud and corruption occurs in procurement transactions, resulting in very significant losses. According to the OECD, US $9.5 trillion is spent on procurement globally every year, equal to 12-20% of the average governments' GDP. The OECD cites estimates that corruption drains 20-30% of this amount, or more than US $2 trillion, annually.[2]

Standard eProcurement systems, even without the installation of the indicators, represent a major advance in the efficiency and integrity of procurement procedures, streamlining the process, reducing its cost and eliminating many opportunities for human interference and mischief. A 2016 article in The Economist reported that:

> *"… For more than a decade, [the Copenhagen Consensus] has assessed the global costs and benefits of different development schemes … The winner, yielding a fantastic $663 in benefits for every dollar spent, is digital procurement. … One study suggests that eProcurement cuts the price of contracts by about 12%. Because switching to online bids is fairly cheap, the assumed returns are huge."*[3]

The indicators can further enhance the benefits of eProcurement by among other things:

- Blocking non-compliant or improper procurement transactions, such as bids from companies on ineligible lists or bids received after the bid deadline;
- Providing instant alerts of possible fraud, prioritized by importance and level of risk, *before bids are evaluated, contracts are awarded or payments disbursed*, for the first time effectively making a fraud detection system a fraud prevention mechanism*;*

[2] https://www.oecd.org/gov/public-procurement/Methodology-Assessment-Procurement-System-Revised-Draft-July-2016.pdf; https://www.oecd.org/cleangovbiz/49693613.pdf

[3] The Economist, Developing Bangladesh, How to Spend It, An Ambitious Attempt to Work Out the Best Use Scarce Resources," May 7, 2016; https://www.economist.com/finance-and-economics/2016/05/05/how-to-spend-it

- Instantly reviewing 100% of all transactions, rather than limited audit samples as used in standard audits;
- Reviewing transactions in a thorough and more effective manner than human auditors can;
- Permitting detailed, real time remote monitoring by oversight agencies, which is not currently feasible in paper procurement transactions; and
- Creating detailed audit trails and digital evidence for auditors and investigators.

In addition to procurement professionals, the Indicators can be used by:

- Auditors conducting procurement compliance audits or forensic audits of suspected wrongdoing;
- Investigators conducting procurement fraud investigations. The Indicators are particularly useful to evaluate the validity of whistleblower reports of misconduct and to focus a subsequent investigation;
- Competition Agency personnel responsible for the detection and prevention of cartel activity and bid rigging violations;
- Development agency personnel involved in the oversight of procurement procedures by borrowers. These officials can receive real time reports of possible misconduct at the same time and in the same details as those received by local procurement officials;
- NGOs involved in the review of "Open Contracting Data" for indicators of fraud, waste or abuse.

On-site or on-line training and instructional materials on how to interpret the reports and follow up on the reports should be provided.

2. How do red flag indicators work?

As noted above, the indicators are computer algorithms that identify red flags of possible fraud, waste, abuse and inefficiencies in tenders and purchasing transactions. The red flags are then matched to their potential related schemes and scored to measure the level of risk. Red flags are not conclusive evidence of fraud but are pointers or symptoms of possible misconduct.

For example, in tenders the indicators may identify bids submitted by different companies that are an exact percentage apart, indicating collusion, or identify bids from debarred bidders. In purchasing transactions, the indicators may identify invoices that do not match the values on the related purchase order, or which greatly exceed the average amount of prior invoices. Much more sophisticated tests can be run, of course, including algorithms that are "learned" by Artificial Intelligence and Machine Learning systems from the analysis of the procurement data and previous tests. (For examples of red flags and the related schemes that can be detected see Appendix A, below). The indicators can be tailored to the available data and the particular risks encountered in different procurement environments.

The initial tests run on the procurement data can be followed by on-line background checks of the firms and individuals identified in the data analytics. These checks, which can be automated as part of the indicators system or conducted separately by accessing relevant online databases, often have proven to be equally effective to identify potential fraud. They include:

- Confirmation of the existence, legitimacy and ownership of a bidder through review of business and tax registrations;
- Information from business reporting services (to compare to the information contained in bids);
- Reverse address and high-risk address checks, to identify bidders located at non-business addresses; and
- Politically Exposed Persons (PEP) and corporate debarment lists reviews.

Further follow up steps can be included in on-line or standard handbooks that can accompany the programs. An example of follow up steps that can be run by investigators can be found at https://guide.iacrc.org; https://guide.iacrc.org/proof-of-common-schemes.

3. Types of reports generated by red flag indicators

The indicators can produce useful reports in the following categories, ranging from simple statistical reports to alerts of potentially fraudulent transactions:

- Significant procurement statistics. For example, the number of contracts awarded to certain contractors by certain approving officials, or the average cost of certain procurements, followed by "outliers" significantly outside those parameters.
- Economy and efficiency indicators. For example, the verification of the selection of the best product for the best price or the failures to do so, as well as the failure to collect available discounts and rebates from vendors, etc.
- Compliance reports. For example, contracts in violation of procurement rules, such as the acceptance of bids from debarred companies or sole source contracts above the sole source limit.
- "SPQQD" reports. SPQQD refers to "Selection, Price, Quantity, Quality and Delivery" Indicators that can point to fraud, waste or abuse. An obvious (but common) example is the frequent, improper selection of a vendor that charges higher prices and delivers substandard product, which points to a kickback scheme.
- Fraud, waste and abuse reports. These include reports of the possible schemes listed above and in Appendices A and B.

When run proactively, the reports can appear as instant "pop up alerts" on an eProcurement portal or as automatically generated emails directed to designated procurement or audit personnel. The reports can contain recommended quick follow up steps to help determine whether fraud, waste or abuse is in fact present and can provide administrative reporting requirements.

4. Types of schemes that can be detected or prevented by governance filters

Among the more common and costly procurement fraud and corruption schemes that can be detected or prevented by the indicators are:

a) Collusive bidding by contractors: this refers to secret agreements by bidders or suppliers to divide work and artificially inflate prices, often with the complicity of government officials.

b) Bid rigging: Improper manipulation of the bidding or vendor selection process to favor certain suppliers and exclude others.

c) "Shell company" vendors: vendors secretly owned by procurement or purchasing agency officials. These "companies" often operate as brokers that add no value to the transactions and receive a disproportionate amount of orders and provide substandard product at high prices.

d) Phantom vendors: "ghost" suppliers, set up by purchasing agency insiders that submit fictitious invoices that are paid as part of schemes to embezzle funds.

e) Purchases for personal use, resale or diversion: a very common abuse that can be quite costly if not adequately monitored and controlled.

f) False, inflated and duplicate payments: another quite common schemes that can expand and be quite costly if not controlled. Such invoices can be submitted and paid in error or deliberately with an intent to defraud.

As noted above, the indicators identify potential schemes by highlighting significant red flags of their presence. For example, the primary red flags of Collusive Bidding, Bid Rigging and Phantom Vendors include:

a) Collusive Bidding:

- Different bids from the same IP address
- Bidders with same contact information
- Unusual bid patterns, e.g., bids an exact % apart
- Sequential bid securities
- Same bidders rebid in same order

b) Bid Rigging:

- Procurement official's contact information is same as bidder's contact information
- Shorter notice to submit bids than rules require
- Sole source awards greater than sole source limits
- Multiple purchases just below procurement threshold
- Award to only one evaluated bidder
- Award to other than the low bidder

c) Phantom Vendors (Ghost Suppliers):

- 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 employee record matches vendor record
- "Fuzzy match" vendors with different bank accounts
- High number or percentage of sequential invoice numbers
- Broken sequence invoice numbers

The presence of a significant number of these red flags would be a strong indication that a scheme is present. More detailed analysis of the data and other follow up steps can then be taken to confirm or exclude the presence of the scheme. More complete lists of the red flags for all six of the schemes listed above are set out in Appendix A, along with the data required to detect them. Other common procurement schemes and inefficiencies that can be addressed by indicators are listed in Appendix B.

5. Scoring of corruption risks

The risk score refers to the risk to the procuring entity and can be calculated by that entity. Scores can be assigned to each indicator or pattern of indicators according to their likelihood of occurrence and the perceived risk level. The likelihood of occurrence primarily depends on the number and nature of the red flags: several red flags are, of course, usually more significant than a single indicator, and some red flags, such as a bidder being listed on an excluded party list, or bids from supposedly different companies submitted from the same computer, are more significant than others.

The perceived risk level refers to the operational, reputational and financial damage that a scheme might cause if it is in fact present: a possible collusive bidding case in a $100 million procurement would present a higher risk level than false invoices for office supplies. The likelihood of occurrence depends primarily on the number and strength of the red flags detected.

The scoring system might be devised by a committee of procurement, audit and operational personnel based on their prior experience and knowledge of the entity's operations and markets. Its primary purpose is to allow the entity to prioritize its responses to the issues raised by the fraud filters, which might otherwise overburden the response team.

6. Measures to limit "false positives"

Dealing with "false positives" – red flags of potential irregularities or fraud that have an innocent explanation – is one of the primary difficulties in implementing any effective digital fraud detection programs. False positives are particularly disruptive if the fraud detection algorithms are too general or are not tailored to the risk environment being examined.

False positives can be reduced by the following measures:

- Identify unambiguous indicators, such as different bids from bidders on a debarred list;
- Identify and prioritize other strong indicator, such as bids from different bidders that are an exact percent apart and sequential bid securities;
- Identify repeat transactions, such as a high number of split purchases by the same procurement official from the same supplier; and
- Identify transactions with multiple indicators, such as a high number of red flags associated with a single purchase.

Another important factor in reducing false positives is to link the indicators to reports of potential fraud, such as whistleblower complaints. The indicators can be used to help verify or rebut a complaint.

7. What are the requirements for successful implementation of the indicators in eProcurement systems?

The most important factor in installing the indicators in eProcurement systems is access to the data required to run the algorithms. As mentioned before, although most of this data is readily available in any procurement environment, it still must be collected and stored in a manner accessible to the Governance Filters.

Early planning for the integration of the indicators is, therefore, quite important, as the planning stage will include the decision as to what data the eProcurement system will collect and store, which in turn will decide what indicators can be run. Existing eProcurement systems that did not incorporate this planning can be modified to acquire the necessary data and install the indicators, but at considerable additional cost and difficulty.

For example, in Indonesia (see page 9, below) planning for an eProcurement system was complete and implementation had begun before the procurement agency became aware of the benefits of the indicators. As a result, the system included only purchasing and receiving information, and not invoice and payment information. Invoice and payment information could have been included but was considered unnecessary. Since most indicators of fraud in purchasing systems rely on invoice and payment information, the utility of the indicators was severely constrained. Adding the missing data at the then current stage of development would have been disruptive and costly, so the developers decided to wait until an upgraded version was delivered to add the invoice and payment indicators.

Data outside the procurement system can be imported if other tests are desired, such as matching the contact information of purchasing employees to bidders or suppliers. Software engineers involved in the installation of the indicators in Indonesia reported that, assuming the relevant data is accessible, and that the eProcurement design allows access to it, the indicators could be installed without significant programming difficulties or additional expense.

8. Examples of red flag indicators in practice

According to a 2014 Transparency International Report, citing a 2013 Price Waterhouse Coopers (PwC) report, the many advantages of eProcurement systems, even without the indicators, have been "under-utilized."

At present it appears that most eProcurement systems are only partially implemented. A typical system, for example, may publish requests for bids on the internet but accept bids in pdf format. This, of course, greatly reduces the utility and benefits of the systems. Exceptions that have been cited as "successful" and more complete eProcurement systems include those in South Korea, Albania, Georgia and Ukraine.

The introduction of Red Flag Indicators also has lagged, probably because of the slow implementation of full eProcurement systems that can utilize them, as well as unfamiliarity with fraud detection procedures among procurement personnel. The same 2013 PwC report found that "although the majority of EU countries have central and/or local databases for public procurement, only half of them query their data about unusual patterns, and only a few develop or use indicators that point to possible cases of corruption. Similarly, only three countries have e-procurement

platforms that contain a module designed for the detection of corruption."[4] The PwC report did not identify the countries.

More current research has revealed the following countries where indicators have been applied.

a) Brazil

The Public Spending Observatory cross-checks procurement data with other government databases. Possible misconduct is identified by "orange" or "red" flags for follow up investigations. Among other Indicators, the system looks for:

- Conflicts of interest by procurement personnel;
- Procurement abuses, such as contract splitting to avoid competitive bidding;
- Unusual bid patterns;
- Bidders with the same address;
- Rotation of winning bidders;
- Contract amendments within one month of contract award.

https://www.oecd.org/governance/procurement/toolbox/search/public-spending-observatory-brazil.pdf

Brazil also has adopted open data policies to help attack corruption. http://webfoundation.org/docs/2017/04/2017_OpenDataBrazil_EN-2.pdf

b) United Kingdom

The UK Competition and Markets Authority developed a tool for use by public sector organizations to detect potential anti-competitive behavior. The system's indicators include, among others:

- Tenders with a single bidder or low number of bidders;
- Price discrepancies: winning price is an outlier, similar bid prices, apparently arbitrary cost calculations;
- " Low endeavor" bids, e.g., bids by the same author;
- Most interestingly, the ability to identify similar text and word count in different bids. Such similarities in bids is the number one red flag of collusive bidding.

The tool has been distributed to almost 90 organizations in the UK and is being reviewed by 29 National Competition Agencies.

https://www.slideshare.net/OECD-DAF/cartel-screening-in-the-digital-era-uk-competition-markets-authority-january-2018-oecd-workshop

https://www.gov.uk/government/publications/screening-for-cartels-tool-for-procurers

[4] https://www.transparency.org/files/content/corruptionqas/The_role_of_technology_in_reducing_corruption_in_public_procurement_2014.pdf; https://ec.europa.eu/anti-fraud/sites/antifraud/files/docs/body/identifying_reducing_corruption_in_public_procurement_en.pdf.

c) European Union

DIGIWHIST - the Digital Whistleblower - offers products devoted to Fiscal Transparency, Risk Assessment, and Assessing the Impact of Good Governance Policies; https://digiwhist.eu. The products include:

- EuroPAM, The European Public Accountability Mechanism, a data collection effort to enhance transparency of public administration and the accountability of public officials; http://europam.eu
- Opentender, a platform that allows the user to search and analyze tender data from 33 jurisdictions; https://opentender.eu/start
- MET, Monitoring European Tenders, another tool to assess the risks in European tenders; https://monitoringeutenders.eu

The Government Transparency Institute provides big data analytics to auditors to identify and prevent fraud and corruption in public procurement; http://www.govtransparency.eu

d) South Korea

South Korea has instituted "BRIAS" – the "Bid Rigging Indicator Analysis System." According to a 2016 OECD report, BRIAS looks at bid prices (as a ratio compared to a reference price), the number of participants and the competition method, and applies a formula that generates a potential bid-rigging score. A significant score leads to the collection of more information from the procurement system, followed by a referral for investigation if deemed warranted.

The OECD report found that the results "have been limited: only three cases initially identified by BRIAS have led to findings of guilt." This is attributed to competition from more traditional whistleblower reporting system, but it may also be the result of the relatively limited categories of data – price, number of participants and competition method – the system initially collects. In contrast, a list of numerous data points recommended for collection for specific schemes is contained in Appendix A.

Interestingly, the OECD report noted that "during the period of [BRIAS] operation, voluntary reporting by cartel participants has increased significantly, and some of this increase is attributed to the raised awareness and fear of being caught generated by the implementation of the BRIAS system."[5]

e) Indonesia

The Red Flag Indicators program in Indonesia referred to in the previous section was developed by the Indonesian National Procurement Agency (LKPP), financed by the US Millennium Challenge Corporation (MCC) and implemented with the assistance of PwC and international and local IT firms.

In addition to the eProcurement system discussed above, the program involved the planned installation of the indicators in the government's database of historic procurement information. The indicators to be installed include the following, with more planned to be introduced later:

[5] https://www.oecd.org/governance/procurement/toolbox/search/korea-bid-rigging-indicator-analysis-system-brias.pdf

1. Recommended contract award to other than the low bidder
2. The low bidder withdraws, followed by award to the second low bidder
3. Bids from different bidders:
    a. have the same business address, telephone number or email address
    b. are from the same IP address
    c. are submitted with ---- seconds/minutes (adjustable) of each other
    d. are identical (including line item bids)
    e. are an exact % apart (including line item bids)
4. 6-9-17 bid pattern (second low bid 6% higher than low bid, third low bid 9% higher, fourth low bid 17% higher)
5. Total or line item bid prices equals cost estimates (or within --- percentage (adjustable))
6. High prices bids: bids --- percentage (adjustable) above cost estimate
7. Less than 30% of companies that bought bid packages submit bids

The following collusion red flags were discovered in Indonesian procurements during the development of the project:

1. Rotation of winning bidders in large infrastructure tenders
2. Different bidders submit "ping ponged" bids for identical different lots or in similar tenders, e.g.,

BIDDERS	LOT A Bid (Specs same as Lot B)	LOT B Bid (Specs same as Lot A)
Company One	$100	$300
Company Two	$300	$100

3. Different bidders submitting bids from the same IP address
4. The same Bid Evaluation Committee members select the same companies a disproportionate percentage of times
5. Other collusive bidding Indicators listed in Appendix A also were discovered in Indonesian contracts in previous investigations.

f) Switzerland

The Swiss Competition Commission (COMCO) has conducted significant research on the digital detection of collusive bidding and bid rigging. Although not directly linked to eProcurement, such

research has identified useful indicators that can be included in eProcurement systems and run on a proactive, real time basis.[6]

For example, COMCO identified the following recurring patterns in its cartel investigations:

1. The range of bids (from highest to lowest) was lower in tenders in which collusion was found, i.e., the highest and lowest bids tended to occur within a 10% window. In similar tenders in which collusion was not found the typical range of bids was in a 20% window;

2. There was a wider gap between the lowest and second lowest bids (e.g. 3.5 % difference) than between the higher bids (e.g. about a 1% difference). This was attributed to the desire to ensure that the designated "low" bidder would have a sufficiently lower price than the next lowest bidder to survive a higher technical score by the next lowest bidder. (The close distribution of bids by the losing bidders also was different than the patterns detected in non-collusive bids in other cases.)

3. The cases revealed a pattern of the rotation of winning bidders and among the same group of repeat bidders.

The Swiss findings are discussed in more detail at https://www.slideshare.net/OECD-DAF/cartel-screening-in-the-digital-era-swiss-competition-commission-january-2018-oecd-workshop;

https://www.oecd.org/competition/workshop-on-cartel-screening-in-the-digital-era.htm

Other red flags that have been proven to be effective in detecting cartel activity in prior cases are set out in Appendix A, Collusive Bidding, below.

[6] For more information see, http://www.oecd.org/competition/workshop-on-cartel-screening-in-the-digital-era.htm

APPENDIX A

Some of the most common and costly schemes and their red flags that can be detected or prevented by Red Flag Indicators:

- Collusive bidding
- Bid Rigging
- Shell Company Vendors
- Phantom Vendors
- Purchases for Personal Use
- False, Inflated and Duplicate Invoices

The sample indicators in the sections below are prioritized and color coded as follows:

- Indicators in red are the most significant
- Indicators in brown are important but less significant
- A number of indicators for each scheme is the most significant.

Both the "primary data sources" and "other potential data sources" listed for each scheme below should be readily available from any eProcurement system. The primary data requirements refer to the information needed to identify the most significant indicators. Other potential data sources refer to the information needed to identify useful but less critical indicators.

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

Red flags include:

- Different bids from the same IP address
- Bidders with same contact information
- Unusual bid patterns, e.g., bids an exact % apart
- Sequential bid securities
- Same bidder's rebid in same order in later rounds
- High price bids; e.g. bids that exceed the confidential owner's estimate by > 30%
- Pattern of rotation of winning bidders
- Same bidders always bid, win and lose
- Losing bidders become subcontractors
- Unusual bid patterns, e.g., "6-9-17 bid pattern"
- Bids not in conformity with prior legitimate bid patterns
- Distant bidders are cheaper than local bidders

Data Requirements

Primary data sources

- Bidder's address, tele, fax, email, IP address
- Winning and losing bids
- Bid securities
- Owner's cost estimates

Other potential data sources:

- Line item prices
- Subcontracts
- Previous bids

The charts below illustrate bid patterns associated with legitimate bids and bids rigged as the result of collusion among bidders. The top chart shows an irregular but plausible distribution of bid prices from seven bidders. The bottom two charts show bids exact percentage apart, an indicator of collusion.

Sample Graphic Reports of Collusive Bidding Indicators

Blue and orange highlighted bids indicate potential collusion

Jobsite: East African Network Tollroad

Bidder	Bid	Ratios of Bid to Estimate	Winner	Prev Bid
Engineer Estimate	$ 132.7M	-	-	-
Barrytron	$ 130.9M	-1.4%	-	-
Tessier-Ashpool	$ 135.8M	2.4%	3.8%	-
Stay Puft Corporation	$ 136.6M	2.9%	4.3%	0.5%
Barrytron	$ 138.5M	4.4%	5.8%	1.4%
Galaxy Corp	$ 140.8M	6.1%	7.5%	1.6%
123 Warehousing	$ 144.1M	8.6%	10.1%	2.4%
Spade and Archer	$ 157.1M	18.3%	20.0%	9.0%

Jobsite: Rila motorway Development

Bidder	Bid	Ratios of Bid to Estimate	Winner	Prev Bid
Engineer Estimate	$ 109.3M	-	-	-
Carrys Candles	$ 102.0M	-6.7%	-22.2%	-
General Services Corporation	$ 131.2M	20.0%	-	-
The Legitimate Businessmens Club	$ 137.7M	26.0%	5.0%	5.0%
Flowers By Irene	$ 140.3M	28.4%	7.0%	1.9%
Allied Biscuit	$ 143.0M	30.8%	9.0%	1.9%
United Fried Chicken	$ 145.6M	33.2%	11.0%	1.8%
Acme Corp	$ 148.2M	35.6%	13.0%	1.8%

Jobsite: I-85/West Point Interchange Project (Troup County)

Bidder	Bid	Ratios of Bid to Estimate	Winner	Prev Bid
Engineer Estimate	$ 122.6M	-	-	-
LexCorp	$ 137.8M	12.4%	-	-
Krustyco	$ 141.3M	15.3%	2.6%	-
General Services Corporation	$ 151.5M	23.6%	10.0%	7.2%
Sixty Second Avenue	$ 166.7M	36.0%	21.0%	10.0%
Smith and Co.	$ 183.3M	49.6%	33.1%	10.0%
LuthorCorp	$ 201.7M	64.6%	46.4%	10.0%

BID RIGGING: Improper manipulation of the bidding or vendor selection process to favor certain suppliers to the exclusion of others.

Red flags include:

- Shorter notice to submit bids than rules require
- Sole source awards greater than sole source limits
- Split purchases
- Multiple purchases just below procurement threshold
- Award to only one evaluated bidder
- Award to other than the low bidder
- Unusually high line item bid, followed by change order increasing quantities
- Unusually low line item bid, followed by change order removing or reducing line item
- Winning bid price the same as cost estimate

Data Requirements

Primary data sources:

- Bid evaluation Committee members and bidder contact info
- Winning and losing bids
- Bid notice and due date
- Debarment list
- Procurement thresholds

Other potential data sources:

- Line item bid prices
- Contract date and price
- Change orders and amounts
- Procurement plan info
- Previous similar tender results

SHELL COMPANY VENDOR: Vendors secretly owned by procurement or purchasing agency officials.

Red flags include:

- HR/vendor matches (cell phone numbers, etc.)
- Vendor not on Approved Vendor List
- Sole source purchases above competitive threshold
- Multiple purchases just below competitive threshold
- Split purchases
- Segregation of duties violations (same person orders, approves and receives purchases)
- SPQQD factors present
- Vendor provides variety of disparate goods or services in contrast to existing vendor norms (per vendor codes and product codes)
- Prompt payment in contrast to the existing payment norm

Data Requirements

Primary data sources:

- Vendor master file
- HR master file
- PO, receiving, invoice, payment information
- Procurement thresholds
- Segregation of Duty requirements

Other potential data sources:

- Benchmark prices

- Vendor and product code lists
- Payment date

PHANTOM VENDOR: "Ghost" suppliers, set up by insiders, that submit fictitious invoices as part of a scheme to embezzle funds.

Red flags include:

- Paid vendor not on Approved Vendor List
- HR employee record/Vendor record match
- "Fuzzy match" vendors with different bank accounts
- High number or percentage of sequential invoice numbers
- Broken sequence invoice numbers
- Purchases just below competitive thresholds
- Split purchases
- Benford's Law violations[7]
- Small initial purchase
- Vendor provides hard to verify goods, works or services (per product code)

Data Requirements

Primary data sources:

- Approved and paid vendor lists
- HR and vendor master files
- PO, invoice, receiving, payment info

Other potential data sources:

- Procurement thresholds
- Benford's Law distributions
- Vendor and product code lists

PURCHASES FOR PERSONAL USE, RESALE OR DIVERSION: A very common abuse that can be quite costly if not adequately monitored and controlled.

Red flags include:

- Purchase of inappropriate personal "consumer items" per product code

[7] Benford's Law states that in naturally occurring number sets, the number 1 will occur as the first digit about 30.4% of the time, the number 2 about 17% of the time with the other digits descending in regular order until the number 9 that appears as the first digit about 4% of the time. Prices in invoices, quantities in reports, etc. that do not follow this pattern can indicate fabricated numbers and fraud. See https://en.wikipedia.org/wiki/Benford%27s_law

- Purchased items not in inventory
- Different "ship to" address
- Split purchases
- High number of purchases of certain items susceptible to personal use (laptops, tires, gas, etc.)
- Returns without credits
- Multiple purchases just below thresholds
- Small initial purchase
- Employee has outside business (used to resell or divert products)

Data Requirements

Primary data sources:

- Vendor product codes
- Purchased item product codes
- PO, invoice and receiving records info
- Procurement thresholds

Other potential sources:

- Returns and credits
- Inventory records
- Procurement plan info

FALSE, INFLATED AND DUPLICATE INVOICES: Whether done intentionally or inadvertently this is a common problem that can be quite costly if not controlled.

Red flags include:

False invoices:

- Invoice information does not match PO, receiving or payment information
- Sequential invoice numbers
- Broken sequence invoice numbers
- Outliers in price, quantity
- Benford's Law violations

Inflated invoices:

- Invoice price, quantities greater than the PO price, etc.
- Total payments greater than total invoice amounts

Duplicate invoices:

- Invoices with same number, dates, quantities, item description or amounts

DATA REQUIREMENTS

Primary data sources:

- PO, invoice, receiving and payment information including:
  - Dates
  - Invoice numbers
  - Item number, descriptions
  - Product codes
  - Price and quantities
  - Receiving info
  - Payment amount

Other data sources:

- Benford's Law distributions

APPENDIX B

Some of the additional fraud, waste and abuse schemes and inefficiencies that Red Flag Indicators can detect or prevent include:

- Failure to collect entitled rebates and discounts
- Failure to comply with procurement regulations and best practices
- Change order abuse
- Co-mingled contracts
- Duplicate payments
- Exclusion of qualified bidders
- Failure to meet contract specifications
- False or inflated invoices
- Front loading of contract expenses
- Improper sole source awards
- Leaking of bid data
- Manipulation of bids
- Overpayments
- Rigged specifications
- Split purchases
- Unbalanced bidding
- Unnecessary and excessive purchasing
- Product substitution

Annex 3 Workshop – list of participants

Lista prezenta subact 3.8._worksh

Annex 4 List of system-level indicators

Indicator	Availability of data within SICAP
These could translate in reviewed legal provisions or guidance. In several cases, it could give an indication of irregular behavior by CA.	
Outcome of review procedure (how many procedures are annulled, suspended… etc) *This is an indicator of possible irregular behavior of CA or economic operator*.	Not within SICAP, but available at CNSC
Average number of offers received ○ per each type of procedure ○ per category of procurement (specific types of works, services and supplies, based on the main CPV group) *This is an indicator of possible bad tender documentation, market shortages, targeted specifications etc*.	Yes
Rejection rate of bidders ○ by types of contracts (works, supply, services) ○ by type of procedure ○ per type of sector – assimilated with group of CPV code *This is an indicator of possible bad tender documentation, market shortages, targeted specifications etc. This could also be an indicator of possible irregular behavior by CA.*	Yes
Contracts awarded by the same contracting authority to the same economic operator: ○ by type of procedure ○ by sector - assimilated with group of CPV code *This is an indicator of possible advantage given to a certain tenderer. Corrective measures could be at CA level.*	Yes

Indicator	Availability of data within SICAP
Contracts awarded by contracting authorities based on single offer *This is an indicator of possible targeted specifications and / or advantage to a certain tenderer.*	Yes
Contract value versus actual value *This is an indicator of possible irregularities during contract implementation.*	Yes, the need for the publication of data within the system should be highlighted to the CAs

Competence makes a difference!

Project selected under the Administrative Capacity Operational Program, co-financed by European Union from the European Social Fund