Thwart procurement fraud
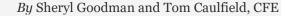
Competitive Advantage

Identifying procurement integrity breaches via data analytics

January/February 2023

By Sheryl Goodman and Tom Caulfield, CFE

As protests raged in Chile in 2020 over the cost of living and inequality, the government sought to procure body cameras for the police to monitor events on the ground. After going through a public bidding process, U.S. telecommunications equipment provider Motorola Solutions won the business to supply 300 cameras at a cost of close to 400 million Chilean pesos, or about $340 each at today's exchange rate. Soon thereafter, those involved in the bidding process found themselves under investigation for irregularities. According to the local press, government officials accepted Motorola's bid even though the company submitted its offer on the electronic procurement portal outside the hours stipulated by the bid rules. (See "El informe de Contraloría que complica a Katherine Martorell, la actual vocera de Sichel, por millonaria compra de cámaras GoPros para Carabineros," El Mostrador, Oct. 15, 2021.)

In early 2021, the scandal intensified after Chile Compra, the entity that runs the electronic procurement portal — known under its Spanish name Mercado Público — revealed that Motorola's cameras had failed to meet some basic requirements — namely an ability to keep recording for at least 120 seconds after being turned off.

The intense scrutiny over the bidding process (and what may seem like a storm in a teacup for some) reflects Chile's seriousness in tackling corruption and its efforts to clean up its procurement process with the help of technology. In the late 1990s, Chile created what was then a first-of-its-kind electronic portal for procurement to improve the efficiency and transparency of public spending. It's been updating the system ever since. The electronic public marketplace brings together all those involved in the procurement process onto one easy-to-find platform. (See "Martorell en problemas: informe de Chile Compra revela que Subsecretaría incumplió bases de licitación para adquisición de cámaras para Carabineros," El Mostrador, Jan. 6, 2021; "Cámaras policiales: testigos revelan presiones para favorecer a Motorola en licitación de Martorell," Nicolás Parra y Felipe Díaz Montero, BioBioChile, March 23, 2022; and "Martorell in trouble: Chile Compra report reveals that Undersecretariat failed to comply with bidding rules for the acquisition of cameras for Carabineros," Archyde, Jan. 6, 2021. Also see "Chilecompra: Using Technology to Deliver Better Value for Public Money," by Rachel Lipson, Harvard, Technology and Operations Management, Nov. 18, 2016.)

This case represents how entities — public or private — can detect and eventually prevent public procurement integrity breaches via data analytics and other types of technology. Other countries around the world have also set up systems that use technology to catch procurement fraud.

[See sidebar: "International examples of data analytics systems".]

These breaches, a major risk to organizations worldwide, can result in unnecessary financial losses, reputational damage, contract delays and even contract terminations. Corrupt officials and internal and external fraudsters love to target public procurement because that's where the cash is, and safeguards are often lacking.

In fiscal year 2020, the U.S. federal government spent more than $665 billion on contracts — an increase of over $70 billion from fiscal year 2019. Half of this increase, or $35 billion, is attributed to spending on medical supplies and pharmaceuticals to treat COVID-19 patients, among other things related to COVID-19. [See "A Snapshot of Government-Wide Contracting For FY 2020," U.S. Government Accountability Office (GAO), June 22, 2021.]

In 2018, the U.S. Department of Defense (DOD) reported to Congress that over $6.6 billion had been recovered from defense-contracting fraud cases from fiscal years 2013 through 2017. In 2020, the DOD Office of Inspector General reported that roughly one in five of its ongoing investigations are related to procurement fraud. (See "DOD Fraud Risk Management: Actions Needed to Enhance Department-Wide Approach, Focusing on Procurement Fraud Risks," GAO, Sept. 20, 2021.)

These breaches, a major risk to organizations worldwide, can result in unnecessary financial losses,

reputational damage, contract delays and even contract terminations.

Violators breach procurement integrity — honest, fair, impartial, transparent and legal contracting — by deliberately and covertly abusing established contracting procedures, policies and requirements. Some examples of breaches are the improper acceptance of late vendor bids, biased technical evaluations during bid scoring, needlessly long delays in contract negotiation or awards, unnecessary limiting of solicitation periods, approving uncalled for contract modifications and competitors submitting complementary bids.

Rule breakers who cause breaches don't always commit contract fraud. For example, some internal employees who knowingly violate procurement policies or guidance might believe established requirements are unnecessarily or overly burdensome. Others might think they're helping their organizations when they perform their contract breaches. (See "Five personality faces of procurement fraud risk," by Tom Caulfield, CFE, CIG, CIGI; and Sheryl Goodman Steckler, CIG, CIGI, *Fraud Magazine*, November/December 2017.) Of course, these breaches are inexcusable, but some well-meaning employees might perform them because of lack of training.

Regardless, organizations can greatly reduce procurement breaches by using robust data analytics and continuous monitoring software. Now it's no longer a question of how technology can ensure procurement integrity, but what are the best ways to incorporate data analytics into our procurement integrity control systems? (A procurement integrity control system is the aggregate of the people, processes, procedures and management systems that are designed to provide reasonable assurance regarding the prevention, detection, reporting and capability to respond to procurement abuse, procurement fraud or noncompliance with procurement policy.)

Ways to perform searches for breaches

Open Contracting Partnership (OCP) is an independent, not-for-profit spun out of the World Bank promoting open and transparent government contracting worldwide.

An OCP global literature review showcased a wide and sometimes inconsistent view on the most effective ways to perform analytical searches for questionable breaches in procurements. (See "RED FLAGS for integrity: Giving the green light to open data solutions," OCP.) However, three common points of agreement were identified:

- The need to contextualize.
- The need to incorporate triangulation.
- The importance of data quality and quantity.

(See "G7 commits to open and participatory public procurement reforms essential to ensure trillions of dollars for recovery aren't wasted," Open Contracting Partnership, Sept. 10, 2021.)

Contextualize

Organizations need to develop effective procurement integrity data analytics in the right context. To illustrate, what's a "short" or "long" period for a given procurement task or an

"abnormally high" or "abnormally low" cost? The answer relies on several specific factors, such as: (1) the type of procurement method (2) services or goods provided and (3) the provider's geographical location. For example, in a highly specialized profession like aerospace, a typical solicitation for the building of a satellite may only result in two or three bidders, but a contract for a new web design may result in over a dozen bidders. Under these scenarios, three bids for a satellite could be considered normal. However, a web design solicitation with just three bidders could be flagged as suspicious.

Triangulation

Triangulation is the use of multiple search conditions to identify a single procurement integrity risk. The number of conditions and specific triangulation methods will depend on available data and the ability to group procurement integrity risks into similar categories.

For example, if your analytics is monitoring the total number of sole-source contracts (also called directed procurements) by procurement departments and it identifies one unit noticeably higher by percentage than the others, is that in itself a procurement integrity risk? (As the name indicates, a sole-source contract is procurement through solicitation of a proposal from only one source.) What if the same analytics also included an additional search requirement for any sole-source contracts containing a modification within 30 days after the award — when 30 days is considered abnormal? If these two analytical results are combined, would it now increase the level of accuracy in identifying a more accurate procurement integrity risk?

If a third search condition is also added — such as the percentage of increase in the dollar value of the sole-source contract over its period of performance — we'd surmise that the higher the percentage, the greater the risks. By adding more search conditions, we increase the ability to identify procurement integrity risks more effectively.

Data quality and quantity

The quality and quantity of available data directly impacts the ability to contextualize and triangulate.

The quality and quantity of available data directly impacts the ability to contextualize and triangulate. Quality in, quantity out (QIQO) means that the value of data input influences the value of the results' output. In practice, it means that if the data going into an analytical model is clean and of sufficient size, the resulting work done by the model will be accurate. Creating data analytical searches to identify procurement integrity is challenging enough; doing so with a data sample that's limited in scale and scope could exacerbate miscalculation and identification of false breaches.

Data availability is also critical. Quick, easy and reliable access to automated data is, of course, the single most relevant requirement for the successful implementation of procurement integrity data analytics. The greater the number of datasets, the more comprehensive and advanced the data analytics technique will be. For example, if your data is limited to only collecting vendor information (e.g., a vendor management system) and human capital information (i.e., employee demographics), your data analytics may be restricted to existing relationships among employees and vendors, improper release of bidding information and/or anti-competitive activity of bidders.

Potential integrity breaches

Organizations collect and store enormous amounts of contracting activity data in a digital format, especially with e-procurement systems, so they can perform multitude analytical searches to identify potential procurement integrity breaches, such as:

- A pattern of contract awards followed by change orders that significantly increase the price of the contracts.
- Invoices notably higher than the average cost of similar services and goods.
- Disparity in bid prices greater than a threshold value.
- An existing financial relationship between a vendor and the procuring entity's employee.
- Bid prices dropping when a new or infrequent competitor enters a competition.
- Patterns of anti-competitive cost submissions in bids.
- Invoicing inconsistent with contract terms.
- Unusual percentage of sole-source contract awards.
- Winning bids that don't meet award criteria of "lowest price technically acceptable" (LPTA) when LPTA is required.
- Inconsistent bid evaluation scorings.
- Awards below the competitive bid threshold followed by change orders that exceed such limits.
- Total payment for service is greater than invoice total.
- Wide variation in line-item bid prices among bidders without apparent justification.
- Contract line items remain in recurring contracts that have never been called for in the past, and/or which weren't called for in future contracts.
- Supplier receives multiple single-source/noncompetitive contracts from a single procuring entity during a defined time period.

(Source: "How emerging technologies are helping tackle procurement frauds," by Arpinder Singh and Harshavardhan Godugula, EY, April 11, 2022.)

Analytical techniques

Parameter analytics

Parameter analytics is a technique that uses a limited number of datasets combined in a simple Boolean condition ("true or false," "yes or no") followed by an action. [Boolean conditions are queries that compare two values with each other, e.g., with == or >= (or "equal to" or "greater than or equal to"), and then return the value true or false or yes or no. Those values that are interpreted as true or false depend on the data type.]

A simple example would be: "Is the name of the requester of the goods and that of the procuring official the same? If yes, identify." Parameter analytics and building Boolean conditions will normally start from a known statement: "If the contract is structured for quarterly payments, the maximum number of payments is four (4)." The Boolean condition would be "is the number of payments greater than four?"

Other examples of Boolean conditions could be: "Does any invoice have multiple tax identification numbers?" Or "does any contract have a change order within 20 days after contract award?" Each of these can be filtered as a "true or false," "yes or no" (Boolean

condition) and whenever positive to identify. It's important to remember that data analytics doesn't identify misconduct; it can only identify indicators or questionable breaches, and therefore each may require additional follow-up to determine the true causes.

Distribution analytics

Distribution analytics rely on accurate historical data, known patterns and thresholds. This type of analytics is looking for outliers throughout the procurement data, such as payments by percentage that are higher than prior purchases for the same items or a greater number of contract modifications than that of a similar contract.

These outliers, more commonly referred to as anomalies, can be identified when looking at multiple prior procurement occurrences in addition to those identified whenever the same type of procurement isn't consistent. For example, identify: (1) abnormally short periods between invoice payments (2) a higher number of payments compared to a similar contract or (3) a higher number of purchases under a multiple-award contract for a product compared to a judgmental sample.

Another example is identifying the percentage of sole sourcing performed by a procurement official compared to other procurement officials. All of these are based on a deviation from what's normal. As mentioned previously, develop effective procurement integrity data analytics in the right contexts (i.e., contextualized).

Social network analytics

Use social network analytics, also called "link analysis," to determine relationships among different entities and/or individuals. Organizations design link analyses with the underlying reality that most misconduct occurs among those familiar with each other and who have previously established relationships.

This analytical approach will normally generate web-like graphic displays that visualize and link the types and strengths of connections among organizations or individuals. These connections might include shared addresses, phone numbers, family relationships, company affiliations and other business connections.

Design social network analytics with a strong reliance on unstructured data, such as blogs, video services, discussion forums and others. An example could be using public media networks like Twitter, Facebook and/or LinkedIn to track potentially inappropriate relationships.

Predictive analytics

Predictive analytics is the gold star of techniques because it can forecast a potential future occurrence of improper conduct or noncompliance to policy or improper payments. Predictive analytics can be one of the more effective contract management techniques. However, predictive analytics isn't easy because it requires (1) assigning a numerical value of risk (i.e., risk factor) to individual procurement actions (2) combining the risk factors together (3) comparing results to historical procurement data of the organization and (4) establishing a range of low to high risk. The proper assigning of a numeric value to each risk factor makes this analytical approach difficult.

To give an example, let's start with this analytical model: Using a range of 1 to 10, with 10 being the highest risk, assign a score based on the number of standard deviations on the

number of contract modification (mods) for a similar contract. The higher the percentage of deviation the higher the risk score up to 10. The predictive analytical model would then automatically combine this risk factor with other risks, again between 1 to 10, such as:

- Number of months for the period of performance: The greater the number, the higher the risk.
- Contract value: The greater the amount, the higher the risk.
- Procurement method used: Sole-sourcing and emergency purchasing are always assigned a higher risk.
- Number of follow-on contracts: The higher the number, the greater the risk.
- Degree of complexity of the effort: Low complexity, low risk.
- Prior incidents with a vendor: Five or more prior incidents of poor performance indicate a higher risk.
- Number of days from contract award to the first contract compared to similar contracts: over 40 days, low risk; between 20 and 39 days, medium risk; under 20 days, high risk.

The combined risks will provide a statistical probability of the contract's overall degree of risk, which can be displayed to visually give an "early warning" and an opportunity to determine what follow-up may need to occur. The statistical probability can be visually displayed to identify each of the numerical values for each risk factor, giving a better understanding of the specific risk condition. The visual display can be configured to perform this type of analytics across a division of the organization, a region of the country or a specific type of contract.

Breeding grounds for fraud

Research by the World Bank found that governments around the world spend an estimated $9.5 trillion on goods and services each year. This accounts for roughly one-third of government expenditures and 10% to 20% of total gross domestic product in many nations — more than 14% in low-income countries. This doesn't account for the trillions of dollars spent in the private sector on contracts. (See "GovTech: Putting People First with Simple, Efficient and Transparent Government," World Bank Live, April 13, 2019.)

A procurement system that lacks integrity is the ideal breeding ground for waste of vital resources, misconduct and even worse, fraud. Regular procurement integrity data analytics can provide indications of breaches that organizations can use to determine whether they need to conduct in-depth reviews.

Data analytics is not the end-all solution, but when combined with trained employees — in a setting committed to procurement integrity — its potential is limitless.

Sheryl Goodman and Tom Caulfield, CFE, are co-founders of Procurement Integrity Consulting Services, LLC —a woman-owned small business specializing in developing, assessing and structuring strategies to ensure contracting integrity. The company also assists both domestic and international clients in identifying and mitigating their inherent risk to procurement fraud and abuse, developing analytical strategies and ensuring an environment commitment to procurement integrity. Contact Goodman at sheryl@procurement-integrity.net. Contact Caulfield at tom@procurement-integrity.net.