Procurement and Supply Chain Fraud

How It Happens and How eCommerce Can Improve Controls

Peter Smith
For OFS Portal LLC
24/04/2015
# Table of Contents

Executive Summary .................................................................................................................. 3

Part 1 - What is the problem? ................................................................................................. 4

Part 2 - How does it happen? ................................................................................................. 5

  Phase One - supplier selection ............................................................................................. 6

  Phase Two – Contracting ..................................................................................................... 8

  Phase Three – Contract Delivery and Management ............................................................ 9

One Further Category ............................................................................................................ 12


  Phase One - supplier selection and qualification ................................................................. 14

  Phase Two – Contracting ................................................................................................... 15

  Phase Three – Contract Delivery and Management ........................................................... 16

Conclusions .............................................................................................................................. 17
Executive Summary

In this paper, fraud and corruption will be examined with a particular focus on fraud linked to procurement and supply chain activities.

Fraud not only costs businesses around the world billions every year, it brings real reputational risk to organisations, and when it becomes endemic, can cause severe economic, social and political issues at national level. In order to reduce the risk of fraud (often driven by corruption from inside organisations), it is important to understand why it happens, and the different areas in which it can occur across the entire end-to-end supply chain and procurement lifecycle.

This paper outlines these different areas of vulnerability, looking in particular at each stage of the procurement process, and identifying the different types of fraud that can be perpetrated. That can be by internal fraudsters, external parties or (as is often the case) both internal and external working in collaboration to defraud the organisation. Therefore fraud can take place in terms of choosing the supplier in the first place: in how the contractual terms are agreed; in the delivery phase of the contract or in the invoicing and payment mechanisms that accompany the delivery.

The final section of the paper then looks at the mitigating actions that organisations can take to protect themselves against fraud. Most of those fall under the headings of policies, processes and systems. In particular, eCommerce technology, when supported by the appropriate processes and policies, can prove very useful in terms of making fraud less likely - for instance by providing clearer audit trails and by its ability to control access to the organisation’s payment regime.

As well as control and visibility, eCommerce systems can also improve the speed of access to data if fraud is suspected. Technology also makes the audit process (whether general or fraud-specific) less time-consuming and therefore less expensive, as electronic documents and data can be retrieved, evaluated and managed much more easily than physical, paper-based records.

The overall message is this. As long as there is the potential for fraudsters to extract money from any situation, fraud cannot be eliminated. But by understanding the issues and taking the right steps in terms of process and technology, organisations can greatly reduce the risk that they will be subject to serious procurement-related fraud.
Part 1 - What is the problem?

**Fraud** is defined as deliberate deception to secure unfair or unlawful gain. In business terms, it generally means extracting money or other benefits from an organisation in an illegal manner that disadvantages that business. **Corruption** is defined as dishonest or fraudulent conduct by those in power, typically involving bribery.

So whilst it is clear that they are different activities, there is also a link in that the fraud often relies on corruption. The fraud is driven or facilitated when an individual or individuals within an organisation abuse their power to make that gain. However, fraud can also take place without any need for corruption from within, as will be described later, in which case the perpetrators might be described as simply criminal rather than corrupt (although there could be some philosophical debate there).

Why are these issues increasingly important for major corporations? It sounds like an obvious question, but why exactly are fraud and corruption dangerous and negative for individual organisations and more widely, for entire nations? The most obvious reason, and the aspect that hits the headlines most often, is the sheer financial loss. Whether it is a firm paying out millions to fraudsters who submit fake invoices, or hijack the payments due to genuine suppliers, or countries losing billions (think of the alleged fraud around the Sochi Winter Olympics, thought to have cost the Russian nation some $15 billion), there is often a direct financial loss.

Then there is the reputational effect. At national level, that can be severe and make business less keen to invest in that country. For individual businesses, it can generate a sense of poor controls or competence, or even of systemic or endemic internal corruption. That can make business partners less enthusiastic about working with the firm, staff less keen to join, and customers less likely to buy.

Alongside the cost and reputational issues, there is now an increasingly important regulatory dimension. For example, the Foreign Corrupt Practices Act in the USA and the Bribery Act in the UK have put greater focus on the need for firms to make sure they are not the drivers of fraud and corruption themselves. When a US or European company bribes politicians or executives in the third world to buy their defence equipment, medical devices or machinery, then they are in effect instigating a fraud on the buying organisation.

Finally, there is the wider effect. Where fraud and corruption is common, at organisational or national level, it starts to distort normal business practice and priorities. For instance, consider a supplier to a government (or indeed a private sector firm) that is known to be corrupt. Winning a contract may well depend more on paying the right bribe to the right person rather than producing an excellent tender and delivering a good product or service. So what is the point of investing in improving the business, if a competitor with an inferior product can win the contract anyway through bribery? So this can lead to a downward spiral of corruption leading to poorer and poorer genuine supplier performance. All these factors mean that everyone in business, and anyone who cares about the strength and performance of the government sector, should be concerned about fraud and corruption.

Having established that, in the next section the various common types of procurement-related fraud (in the business world) will be discussed. Bear in mind too, that by definition, this includes what might be described as “sales-side” fraud too. Clearly, any fraud that involves sales people or processes must involve a buy-side party as well.
Part 2 - How does it happen?

There are many different types of procurement-related fraud. Classifying them in some manner helps to understand how the fraud potentially happens, and is helpful in terms of looking at ways of reducing the chances of successful fraud taking place.

Usually, there are three critical factors to consider: the perpetrator(s), the plan and the point of failure. The perpetrator is behind the fraud and either executes it directly or through others. The perpetrator can be an employee or employees of what can be termed the “victim organisation,” or a supplier, an agent who works with the victim, or indeed a third party that has no direct business relationship at all with the victim. The perpetrator can also be any combination of these different parties; so often it is an employee working with a supplier to execute the fraud.

So classification of fraud can be carried out along these lines. It is possible to look at internally driven fraud as a subset, with one or more staff members (who by definition can be considered as “corrupt”) driving the process. Another subset would then be externally driven, with a third category where internal and external work together. The plan and point of failure factors are linked in that often the plan relies on the point of failure. In other words, most frauds take advantage of some weakness in process, technology, policy, systems or a combination of those.

But in terms of thinking about how to protect the organisation, perhaps a more useful classification is to consider fraud in terms of when during the end-to-end procurement process (in its widest sense) the fraud takes place. Actions can then be designed to make such fraud difficult by addressing the various stages of that process. There are three key phases within the procurement life-cycle that can be considered:

- the supplier selection phase;
- the contract negotiation and award stage; and
- the contract delivery / management phase.

At all stages, as the paper covers in greater detail in Part 3, strong “industrial strength” processes and systems can go a long way to reducing the incidence of fraud. It can never be eliminated completely, but the right eCommerce systems, allied to appropriate policies and processes, can make fraud harder to execute and easier to detect. That will undoubtedly reduce the probability that any fraudster will choose to target the organisation.
Phase One - supplier selection

Often, the fraud here is based around a firm winning the contract that really would not do so were it not for the fraudulent activity. There are a number of different ways in which this can happen:

- **Misrepresentation** - the fraud can take the form of a firm concealing the true nature of its business, history or ownership when it bids for the work. That may be because of issues around bankruptcy, ownership by unsavoury characters, or similar factors that might otherwise discourage the buyer from awarding the contract to the firm. Another variant is the use of “fake firms” to create a false sense of competition (the fraudster creates these entities to bid so it looks like there has been a genuine competition where none really existed).

- **Collusion and Cartels** - one of the oldest types of fraud is cartel-related activities. Back to ancient times, there are records of trades people of different sorts getting together to control markets, always with the aim of benefitting themselves at the expense of the buyer, whether that was an end-consumer or other businesses.

| CASE STUDY | The European Commission imposed a total fine of €131 million on five groups – Bridgestone, Dunlop Oil & Marine/Continental, Trelleborg, Parker ITR and Manuli – for participating in a cartel for marine hoses between 1986 and 2007. Yokohama also participated in the cartel but was not fined because it revealed the existence of the cartel. Marine hoses are used to transport crude oil to and from ships for transportation from production sites. The cartel members fixed prices for marine hoses, allocated bids and markets and exchanged commercially sensitive information. The firms regularly met to fix prices and exchange sensitive market information. Cartel members referred to some markets as their "private markets" and agreed upon a dozen or so pages of detailed "cartel rules" to limit their conduct on the market.  

> A classic case of cartel fraud on an industry-wide scale. At any one time, competition authorities around the world are investigating multiple accusations of cartel or monopoly-type behaviour. This is not easy to detect, but advanced spend analytics systems might highlight prices from different providers moving in sync, or not responding to raw material and market price movements.

- **Biased competition** - running a process to determine supplier selection in a manner that is not truly fair and transparent is a major type of fraud, and is extensive enough that it can be sub-divided along the lines of several different mechanisms. Basically, it involves making sure a particular firm wins the contract, usually in return for a bribe being paid to the internal perpetrator by the supplying firm. So usually these cases involve both a corrupt insider and a firm willing to pay a bribe in return for being favoured. The simplest form is where a buyer decides on the supplier without any formal evaluation process or even without any competition, in return for some inducement. This is fraudulent, even if the supplier is in fact the “best” supplier for this particular contract.
• **Biased competition through specification** - moving into somewhat more sophisticated ways of making a fraudulent selection, a buyer, specifier or budget holder may construct a specification that makes it likely or inevitable that the particular supplier will win the competitive process. At the extreme, the supplier may be the only one that can fulfil the specification – something that is seen at times in sectors as varied as defence, software or complex technical equipment.

**CASE STUDY** - India has terminated a £466 million helicopter order with the British-Italian company AgustaWestland following accusations that the firm bribed officials. In a recent statement, India’s defence ministry said it was axing its order for 12 helicopters, a variant of the company’s anti-submarine warfare model, the AW101 or Merlin that has been designed to transport high-ranking officials.

It said: "The government of India has terminated with immediate effect the agreement that was signed with AgustaWestland International Ltd (AWIL) on 8 February 2010 for the supply of 12 VVIP/VIP helicopters on grounds of breach of the pre-contract integrity pact and the agreement by AWIL." Allegations that the company had used middle-men to bribe Indian officials to win the 2010 contract began to emerge last February, with suggestions that a defence ministry specification insisting its new helicopters should be capable of flying at altitudes of 6,000 metres was cut in order to benefit AgustaWestland.

*If this was indeed fraud, it was quite a sophisticated example, depending on a subtle change to the specification in order to favour a particular bidder. That work was allegedly done by the internal party here, in return for inducements offered by the supplier who gained from the process.*

• **Biased competition through tailoring the evaluation process** - instead of tailoring the specification, the internal fraudster might make sure the evaluation process is biased towards their bidding accomplice. So for instance, knowing the favoured supplier has high prices but provides good quality products, an evaluation process is constructed that gives little weight to “price” and a high weighting to “quality.”

**CASE STUDY** – Leonard Francis, of Singapore-based Glenn Defence Marine Asia (GDMA), or “Fat Leonard” as he is apparently known to his friends, is a Malaysian businessman who pleaded guilty in late 2014 month to fraud charges, admitting bribing US Navy officers with “cash, prostitutes, Cuban cigars and Kobe beef.”

This was a decade-long scheme involving tens of millions of dollars in bribes to win hundreds of millions in business and over-payments. The Navy officers were paid in return for favouring GDMA as a supplier of “husbanding agent” services. That involves a range of tasks for ships visiting ports, including arranging for pilots and tugs; customs and catering; dock security; taxis; and food, fuel and supplies. Three U.S> Navy Rear Admirals have been censured and there is likely to be further action against various US naval officers.

*The methodology for this fraud involved a number of the mechanisms discussed here. First of all, GDMA undercut its rivals in bidding processes to win the contracts, helped by insiders who would “put in a good word” on Francis’ behalf. But the bids were so low that the Navy should have questioned whether they were realistic – the first point to note for procurement practitioners generally. Once the contracts were won, more ships were routed to ports where his company worked by the Navy officers involved, which enabled Francis to submit fake or inflated invoices. These invoices presumably were paid either without real checking of the detail, or via approvals from those on the inside of the scam.*
• **Biased competition through information leakage** - another way of favouring a supplier is to leak information that gives the firm an advantage in the bidding process. That may be insight as to the specification or about the bids received from other competing suppliers, to enable the favoured firm to be awarded the tender. This has been historically a fairly common fraud - tipping off a supplier as to the price they needed to bid to win the contract, in return for a bribe of course.

**Phase Two – Contracting**

Having moved through the supplier selection phase, the next critical point at which fraud can take place is during the contract negotiations and in agreeing the detailed terms and conditions:

• **Terms and conditions** - this requires collaboration between an insider and the supplying firm. The two parties then agree terms and conditions that are not truly market-driven or in the buying organisation’s best interests. The insider then receives some payment or inducement to agree to this. Whilst no fraud or corruption has been proved, a recent UK case saw the “buyer” allow a property developer to renege on an agreement to provide socially useful amenities as part of a scheme. (This was stopped by the courts after a challenge as it was deemed to be breaking EU procurement regulations.)

**CASE STUDY** - Three men were jailed over a scam that saw Sainsbury’s supermarket overcharged by nearly £9 million. Two directors at a potato supplier showered the supermarket’s potato buyer John Maylam with gifts and hospitality in return for lucrative contracts. Maylam, 45, from Kent, was jailed for four years at Croydon Crown Court. David Baxter, 50, from Shropshire, was jailed for 30 months and Andrew Behagg, 60, from Cambridgeshire, received a three-year sentence.

Judge Nicholas Ainley said it was "very nearly as serious a case of corruption as I can imagine" that involved Sainsbury's "being bribed with its own money." The investigation revealed that £4.9 million was paid to Maylam using cash from the scam, and the supermarket says it was overcharged £8.7 million.

*A collaborative effort here, and hard to spot; who knows the true market price of potatoes (except for the potato buyer)? But again, better market data and analysis might have highlighted the scam. And an effective contract management system might have shown a lack of competitive process in terms of supplier selection. Finally, were the buyer’s orders signed off and approved by a more senior person? Systemising approvals is a clear good practice process.*

• **Fraudulent Offsets, Local Content Claims** - whilst fraud can start here once the contract is up and running, the seeds are often sown at the contracting stage. For instance, a need for the supplier to show that there is a certain level of “local content” in their work might be agreed – but without any clear contractual mechanism to explain how this will be measured or policed. It may be that the buyer does not really care about local content, but wants it to appear that they are “doing the right thing.” Or a government buyer might stipulate local content (or “offsets” in the defence industry), but accept a bribe in return for not actually checking that the supplier is fulfilling its obligations.
Phase Three – Contract Delivery and Management

In the phase which involves suppliers actually delivering the work, whether that is goods, services or works, there are a vast number of potential frauds that can be executed:

- **Fake invoices** - in these cases, the fraud can come purely from an outside perpetrator, or from an insider, or indeed collaboration as in the example below. Basically, invoices are submitted when nothing has actually been delivered to the buying organisation. A third-party fraudster submitting convincing-looking invoices for “directory entries” or “event sponsorship” is a long-established fraud that relies on poor processes within the organisation rather than internal help. Or it can be an insider creating false invoices, perhaps even using the name of a genuine existing supplier.

- **Volume over-invoicing** - in these cases, the supplier does actually provide some goods or services, but invoices for more than what has actually been delivered. This can apply across absolutely anything that the organisation buys; from a supplier exaggerating the number of hours worked in giving legal advice (“I was thinking about your case in the shower,” as lawyers who record 18 hours of billable time a day tend to claim), or invoicing for more sacks of peanuts than were actually delivered. It can be purely externally drive, or an internal accomplice may smooth the way by authorising receipts or invoices.

- **Price-related over-invoicing** - here, rather than exaggerating the volume that has been supplied, the price invoiced is greater that what is contractually agreed or allowable. Again, this can be committed by the supplier alone, or in collaboration with an insider who can facilitate smooth passage of the inflated invoice.

**CASE STUDY** – The current scandal around Banamex, Mexico’s second-largest bank and Pemex, the Mexican State oil company appears to have invoicing issues close to the heart of the problem. It appears that Oceanografí a, a contractor to Pemex, received funds based on some sort of “fake invoice” process. Whether insiders were involved, and whether the scandal goes deeper into money-laundering and politics is not clear yet. *Invoice fraud can be made much less likely by robust eCommerce-based purchase to pay systems and processes, which can readily provide supporting documentation. Matching purchase orders, goods or services received and invoices, with defined approval workflows and sign-off, can eliminate all but the most complex and multi-participant frauds. Visibility and access across systems here would have made verification of the records relatively easy.*

- **Invoice diversion** - a fraud that has apparently grown in popularity in recent years is “invoice diversion,” whereby a legitimate payment that should go to a certain supplier is diverted to a third party fraudulently. The third party persuades the buying organisation that the payment should be made to their bank account rather than the real supplier’s, and by the time the real supplier finds that its expected payment has not arrived, the fraudster has emptied the account and disappeared.
CASE STUDY - The UK Olympic Delivery Authority (ODA) and the construction firm Skanska were the victims in 2012 of what appeared to be a fairly simple but elegant fraud. The fraudster contacted the ODA at a time when a large invoice payment was due to Skanska for work on the 2012 Olympics construction programme. As the BBC reported:

“He obtained £2.3 million by pretending to be Skanska's finance director and writing to the ODA with a change of account details ahead of a bank transfer. The account details he gave were his own.”

The fraudsters also tried the same thing with other Skanska clients, including Dorset Council, Network Rail and Universal Builders Supply. The reports don’t say what happened there - perhaps their systems were good enough that no money was paid to the perpetrators. But given that the ODA said 95% of the money had been “recovered” one assumes that the ODA did actually make payments. It was always going to be discovered of course - a short time later – one assumes Skansa called the ODA and asked where their money had got to!

This is a classic invoice / payment misdirection fraud. It can be perpetrated purely by the outside party, or in collaboration with an internal party who can facilitate the payment from the inside. Clear controls and systemised procedures on onboarding suppliers and managing their key details would have prevented this fraud.

• **Easing contract terms** - in this case, collaboration between buyer and seller allows the supplier to benefit from a change in contract terms that benefits them. That may be additional contract volume, or it could be relaxation of specification or delivery requirements. In return, the insider receives some benefit from the supplier.

• **Quality of goods (or services)** - this is one of the toughest frauds to prevent or even detect, as the case study below demonstrates. Basically, the supplier delivers something that is of lower quality than it is contracted to provide. The highest profile example of this recently has been the scandal of horsemeat used surreptitiously in meat products such as burgers, with several European countries involved in the dubious supply chain. But there are many other cases, from counterfeit components to temporary staff who do not have the qualifications they claim. Clearly, this fraud can have severe health and safety implications as well as financial and reputational consequences.

Copyright © 2015 OFS Portal LLC
Fig.1 Understanding the Raw Material Supply Chain is Vital

CASE STUDY - In March 2015, a case going back to the early 1990s finally came to the courts. Global trading giant Glencore was ordered to pay $40 million to OMV Petrom SA by a UK court, for fraudulently shipping oil of a lower-than-purported quality to Romania in the 1990s. As the press release stated:

“Marc Rich & Co., later to become Glencore International AG, sold about 32 shipments to Romanian state firms from 1993 to 1996 made up of cheaper crude blends than agreed, and falsified documents, Julian Flaux, the judge in the London court, said in his ruling on Friday. It profited by about $40.1 million from the “deceit,” he said.”

This is an example of a very hard-to-detect fraud – substitution of inferior products for what the buyer believes they are receiving. Whether it is components, food ingredients, or indeed oil, it is often difficult to know without extensive checking and testing exactly what it is that is being delivered. However, even in this case, appropriate technology in document management and quality systems can help to make the quality processes more robust and usable.

- Stealing products - some of the frauds described here are complex in nature. But sometimes very simple examples still occur and hit the headlines. In a recent case, a woman who worked for the UK’s National Health Service was convicted of stealing over £100,000 worth of printer toner cartridges. She simply ordered them from the supplier, and when they arrived, she took them home, and sold them on eBay! Amazingly, it took some years for this to be detected, and it was her eBay account that gave it away eventually, not the internal data that might have shown the hugely out-of-line spend that her department was making on toner cartridges.
One Further Category

It is worth mentioning one other area for fraud that does not perhaps fit neatly into the above. That is around the use of agents and middle-men of various types in the supply chain, which is often an area for potential fraud. That can include the role of agents in “local content” and “offsets” processes, where they often help disguise the fact that money designated for positive purposes is ending up in the hands of corrupt politicians or executives. And firms also have to be aware that their agents may be committing fraud or encouraging corruption within their supply chain.

For instance, it is a fact that free movement of goods in some countries unfortunately relies on payments to certain people such as customs officials or security services. If agents are paying those bribes in effect on behalf of the buying organisation, perhaps to ensure goods are moving through the supply chain in a timely manner, is there some culpability there, even if the agent is operating largely under its own discretion?

Fraud Methodology - Summing Up

Certain conclusions are clear in looking at both theoretical basis for fraud and corruption and the real-life examples that are featured here.

1. **It is impossible to stop completely fraud and corruption.** Wherever there is money changing hands in a legitimate manner, some individuals will be tempted to try and extract benefits improperly, and there are many different ways in which that can be attempted.

2. However, in the majority of cases, **robust technology, systems, processes and policies will make fraud much less likely and will stop some types of fraud completely.** Just reading some of the cases here, it is easy to see how basic processes and controls would have stopped matters developing to the point of fraud.

3. Other types of fraud are harder to eliminate completely, but even in these cases, **the appropriate processes will make live much more difficult for the aspiring fraudsters.** And organisations that do not take sensible precautions are likely to see a higher risk of fraud as others do take the appropriate steps - the fraudster will be attracted to the easier target.

4. **eCommerce technology has an important role to play** in reducing the chance of fraud and detecting it when it does occur. That includes spend analytics, eSourcing and the whole range of eProcurement purchase-to-pay systems, as the various case studies highlight. It makes analysis of data quicker and easier; provides systemisation of approvals and embeds appropriate “separation of duties” structures; opens up competition and provides much improved audit trails.

Copyright © 2015 OFS Portal LLC
**Fig. 2 Types of Procurement Fraud**

<table>
<thead>
<tr>
<th></th>
<th>Supplier-driven</th>
<th>Staff-driven</th>
<th>Conspiracy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Supplier selection</strong></td>
<td>• False information about firm / capability</td>
<td>• Seeking bribes for favouring suppliers</td>
<td>• Leaking of info re bid</td>
</tr>
<tr>
<td></td>
<td>• Disguising past track record</td>
<td>• Biased supplier selection</td>
<td>• Communicating competitive bids</td>
</tr>
<tr>
<td></td>
<td>• Offering bribes to influence selection</td>
<td>• Adjusting specifications to suit bidder(s)</td>
<td>• Tailoring the specification</td>
</tr>
<tr>
<td><strong>Contracting</strong></td>
<td>• Offering bribes to ease Ts and Cs</td>
<td>• Seeking bribes</td>
<td>• Agreeing unfavourable terms for buying organisation</td>
</tr>
<tr>
<td></td>
<td>• Concealing source of supply (passing off)</td>
<td>• “Commission” payments from suppliers</td>
<td>• Misuse of &quot;local content,&quot; offsets etc.</td>
</tr>
<tr>
<td></td>
<td>• Legal transgressions</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Contract management</strong></td>
<td>• Fake invoices</td>
<td>• Staff submitted fake invoices</td>
<td>• Over-payment against contract (pricing)</td>
</tr>
<tr>
<td></td>
<td>• Over-invoicing</td>
<td>• Stealing product</td>
<td>• Under (or zero) delivery (or over invoicing)</td>
</tr>
<tr>
<td></td>
<td>• Non contract pricing</td>
<td></td>
<td>• Quality slippage</td>
</tr>
<tr>
<td></td>
<td>• Invoice diversion</td>
<td></td>
<td>• Additional volume to contract</td>
</tr>
<tr>
<td></td>
<td>• Local content misinformation</td>
<td></td>
<td>• Agreeing better terms e.g. price increases</td>
</tr>
</tbody>
</table>

Figure 2 (above) shows the fraud types discussed, classified both by the procurement process stage and whether they are internal, external or collaboratively driven (some can be more than one of those types as discussed earlier). And in the next section, some of the key measures that can and should be taken to reduce the risk of fraud will be outlined.

**Part 3: How to Reduce Fraud – Procurement Processes, Systems and Tools**

Based on the different stages of the procurement process described earlier, there are sensible steps that can be taken to protect the integrity of the organisation. Most are based on three key factors: having effective procurement and spend management **policies** in place; using appropriate and robust **processes**; applying the right **technology** to support and manage those processes.

Referring back to the last section, the three stages can be considered again in terms of those steps.
Phase One - supplier selection and qualification

At this initial stage of the process, eSourcing tools and technology, including those that include project management and collaboration capability, can be used to help prevent fraud and corruption. Supplier information management tools also play a key role in verifying and qualifying suppliers.

The aim is to stimulate fair and open competition, and as in all of these actions, a clear procurement policy is a necessary starting point. That needs to cover when competition should occur, the rules for contract award without competition, how opportunities will be advertised and the minimum number of bids that will be sought at different spend levels. It also covers supplier qualification, ensuring that supplies are who they say they are, are qualified to do the work for which they are bidding and generally are firms with whom the buyer is happy to do business.

Other worthwhile mitigating actions include the following:

- Developing the requirement and specifications in an open and transparent manner; ensuring that internal sign-offs and approvals have multiple sign-offs to ensure one person cannot skew the requirement towards a particular supplier.

- Similarly, ensuring that the design of the evaluation process has wide stakeholder involvement to ensure it too is fair and transparent. Suppliers should always be informed how tenders will be evaluated.

- Always looking to achieve strong competition for any significant contracts. Tools and technology such as supplier networks or on-line marketplaces can help here, providing a “ready-made” universe of potential suppliers who may be capable of bidding and being good suppliers. That also applies to contract renewals. Contracts should not just run on for years and years without re-competition (that might have exposed the Sainsbury’s potato fraud described above).

- Ensuring that there is a clear audit trail of communication with suppliers, so there is less chance of one receiving favourable treatment, and that all potential bidders are treated in a similar manner. eSourcing technology can help to ensure this happens and that a good audit trail is maintained. Bidders should be told how their tenders will be evaluated and feedback provided to the unsuccessful applicants; this all encourages transparency and openness.

- Protecting the integrity of the bid or tender. In the pre-digital world, “tender opening ceremonies” tried to ensure that no-one had the chance to communicate bids until all were received. Technology can now mimic that process more effectively.

- Checking suppliers to make sure they are genuine firms, that they “are who they say they are” and that they don’t have a track record of illegal or inappropriate behaviour (which can apply at corporate or director / owner level). Using pre-verified suppliers, or checking through various tools that are available can mitigate risks here.

- Placing controls on onboarding, so that those firms who are actually going to be suppliers go through more rigorous checks before they are accepted onto the supplier master file (or equivalent) that will enable them to be paid.

Copyright © 2015 OFS Portal LLC
Phase Two – Contracting

- At this point, a clear record of what is being agreed contractually is essential, and for larger organisations, a contracts database or contract lifecycle management system is essential. Compared to paper-based processes, the ability to develop, check, authorise and interrogate contracts is an order of magnitude easier once this is automated and systemised.

- Contract management systems can now also help and provide input to contract authoring, which can help to ensure that all key standard terms and conditions are at least considered. Systems can also support an appropriate level of sign-off and approvals management for contracts.

- That point is key. There should be more than one person who is involved in or at least aware of the key contractual terms being agreed. As in many elements of the procurement process, the concept of separation of duties is important, to make sure that there are checks and balances and that no one person holds too much power in the process.

**CASE STUDY** - The Kenyan government has recently introduced an electronic public procurement and payments system as part of the Integrated Financial Management Information System (IFMIS). “Through automation of public financial processes, the IFMIS has provided an interlinked system of internal controls providing clear audit trails and identification of the originator of all transactions,” said President Uhuru Kenyatta.

The system has automated the tendering process, and brought in controls for the registration and qualification of suppliers. Online approvals and automated workflow have streamlined the whole procurement process, and helped to reduce timescales as well as promoting transparency and accountability. Suppliers can submit and track invoices and payments online, and both routine auditing and any particular investigations can be carried out much more quickly and easily than was possible when the process was largely manual and paper based.

*Many governments and public bodies see eCommerce as a major element of their fight against corruption in public procurement activities. But exactly the same principles are applicable to private sector firms, particularly large businesses and those operating in areas where corruption is prevalent.*
Phase Three – Contract Delivery and Management

The long list of potential fraud mechanisms given earlier shows how vulnerable organisations can be to fraud during the delivery phase of a contract. And yet, many of the routes can be closed off by taking a few precautions, simple in context but sometimes harder to implement for operational reasons. These actions usually rely on technology to support the process, including workflow management systems, purchase to pay and eInvoicing automation, and spend analytics to allow analysis of key data.

It is not impossible to implement a purely manual system including the same processes, but it is much easier where the transactional process has been standardised and systemised.

Here are the key steps to be considered:

- A “no purchase order, no pay” policy, along with appropriate checks at key stages, is the single most valuable way to reduce the potential for procurement fraud - and indeed to drive good procurement processes generally.

- “No PO, no pay” means that invoices are only paid if there is an accompanying purchase order, properly authorised, which the invoice details match in terms of prices, volumes, maximum spend limits or similar constraints. This cuts off the possibility of random invoices being paid, (“you subscribed to this directory”) or higher-than-agreed prices or volumes being submitted on invoices.

- Where it is impossible to fully specify the goods or services as part of the purchase order, there should be supporting documentation to verify exactly what it is that has been provided by the supplier. The “separation of duties” issue (see below) needs to be considered here as well; for major purchases, multiple verification is sensible.

- Organisations should certainly implement “two-way matching” – which ensures invoices match purchase orders. “Three-way matching”, where delivery details form the third leg of the control process, has some practical issues (for instance, confirming receipt of services is less straightforward than confirming that goods have been delivered) but when coupled with contract price validation, introduces a further constraint on fraud.

- The other key principle is “separation of duties.” Put simply, the same person, even if very senior, should not fulfil all the key roles within the procurement process. If the same person can choose the supplier, agree the price, confirm delivery and sign the invoice, then there are obvious risks.

- Checks and balances in terms of sign-offs and approvals must be built into the workflow process; again, this is made easier by technology and automation that avoids the need for pieces of paper to fly around the organisation. The best systems for instance now allow approvals via mobile devices, have automatic routing, reminders and other features to make processes robust but easy to use.

- There must be controlled processes around any changes to supplier payment details in particular. (See “invoice diversion” above to understand why). That should include formal confirmation back from the buying organisation to the supplier before any change is made.

Underpinning all of this is the need for a robust spend management policy, covering all the aspects from selection of suppliers to use of the transactional system, approvals and (an area for which there is not enough space to
discuss fully here) a code of conduct covering appropriate ethical behaviour with suppliers and other third parties. As well as the formal policy, organisations should develop a culture where fraud is not tolerated, which means that strong compliance management is also required, which covers the auditing regime, and the steps that will be taken if staff are found to have transgressed.

As well as conventional audit, spend analytics is another useful tool in terms of spotting potential fraud. For example, that might highlight unusual spend patterns in certain cost centres, large usage variations between business units, or highly concentrated spend with a certain supplier. Indeed, the use of analytics and the growing computing power behind “big data” to detect fraud is another whole topic in itself.

Conclusions

Fraud and corruption cannot be eliminated from any organisation. And given the vast sums of money that flow through supply chain and procurement-related activities, these areas will always be a temptation for the aspiring fraudster to look for new ways of making illegal gains. Those opportunities can arise at every stage of the supply chain and procurement process, and organisations need to be smart and vigilant to reduce the chances of being victims of fraud.

Fortunately, there are also many steps that can be taken to achieve this. By understanding the issues and taking the right steps, organisations can greatly reduce the risk that they will be subject to serious procurement-related fraud.

eCommerce technology has greatly helped in this regard, including spend analytics that can detect unusual spend patterns, systems that support more transparent processes at supplier selection stage, and well controlled purchase to pay eCommerce systems and processes (such as “no PO, no pay”). But as well as the right processes and technology, organisations need robust spend policies, well communicated and then enforced, in order to instil a culture of propriety and appropriate behaviour amongst staff. And whilst it is better to put steps in place that make fraud unlikely to happen, appropriate audit processes, even if they take place after the event, are another deterrent to the fraudster.

So policy, process and technology are the watchwords. No organisation can make itself absolutely fraud-proof, and no doubt fraudsters will keep coming up with new and innovative ways to cheat their way to extracting cash, but executives can go a long way towards protecting themselves and their organisations by focusing on those three key factors.
About the Author

Peter Smith, Managing Director, Spend Matters UK / Europe

Peter has over 25 years experience in procurement and supply chain as a manager, procurement director, consultant, analyst and writer. He is Managing Editor of Spend Matters Europe, and with Jason Busch, the founder of Spend Matters in the US, has developed Europe’s leading web-based resource for procurement and industry professionals. Peter worked as Procurement Director for the NatWest Group, the Department of Social Security (the DSS), and the Dun & Bradstreet Corporation, and held senior positions in the Mars Group during his management career. He has an MA in Mathematics from Cambridge University, is a Fellow and was 2003 President of the Chartered Institute of Purchasing and Supply, and his first (co-authored) book, “Buying Professional Services”, was published by the Economist Books in 2010. Further information on this topic and others, and links to the other sites in the Spend Matters Group, can be found at http://spendmatters.com/uk/ or Peter can be contacted at psmith@spendmatters.com

Reproduction of this publication in any form without prior written permission is forbidden.
OFS Portal, LLC

1330 Post Oak Blvd., Suite 2025,
Houston, TX 77057 USA
Phone: +1 832 681 7300
Fax: +1 832 681 7301

Europe ● Africa ● Middle East ● Far East
+44 (0) 7780 7007872
Mexico
+52 55 8421 7903
Web site: www.ofs-portal.com

About OFS Portal LLC
Headquartered in Houston, OFS Portal, LLC (www.ofs-portal.com) is a global member-based group of upstream oil and gas suppliers and service providers at the forefront of oilfield eCommerce. With eCommerce focused on helping buyers to digitize their supply chain, OFS Portal promotes cost-effective approaches to make eCommerce a reality for both buyers and sellers. OFS Portal works with global standards organizations to converge or develop open and royalty free eCommerce standards for use in the upstream oil and gas industry.

Electronic catalogs are provided in standard format at no cost to OFS Portal members' customers. OFS Portal operates with a non-profit objective. Success is measured by the members' ability to reduce costs, increase internal efficiencies and optimize customer service. OFS Portal members include: Baker Hughes, Cameron International, Halliburton, Schlumberger Oilfield Services, Select Energy Services, Trican Well Service, GE Oil and Gas, and Weatherford International.

Chris Welsh
OFS Portal, LLC
CEO
+1 (832) 681 7318
cwelsh@ofs-portal.com

Dave Wallis
OFS Portal, LLC
Director – Eastern Hemisphere
+44 (0) 7780 700782
dwallis@ofs-portal.com

Copyright © 2015 OFS Portal LLC