Principles of Procurement Fraud Prevention

Five ways to combat the new wave of procurement fraud

By Dave Verma,
In association with FISCAL Technologies

CPD CERTIFIED
The CPD Certification Service

Introduction.

Fraud is an ever-present threat to organisations globally, with procurement fraud being a significant concern. According to recent data, 51% of organisations have experienced fraud in the past two years[1], highlighting the persistent nature of this issue. The financial impact is staggering, with businesses losing approximately $50 billion annually due to employee theft alone[2]. The fraud detection and prevention market is expected to grow at a rate of 28.22%[2], reaching a valuation of $200.37 billion by 2030[3], driven by increasing digitisation and the adoption of AI and data analytics.

Unfortunately, the procurement profession is not immune to the technological and social factors driving this increase in fraud. In fact, procurement may be uniquely vulnerable given its large processing volumes, diverse suppliers, staffing challenges, high-value transactions, and—in some cases—entrenched attitude that the problem is intractable and simply a "cost of doing business."

However, Dave Verma doesn't view procurement fraud as inevitable or unpreventable. As one of the UK's most experienced fraud investigators, Dave assists a wide range of clients in developing an anti-fraud culture, enhancing corporate standards and procedures, and providing bespoke training for investigators, human resources, and lawyers. Beyond policy development, Dave works with organisations to conduct complex interviews and investigations when necessary, and helps create disciplinary and evidential packs for the police, civil recovery, and prosecutions.

Working with both corporate clients and public-sector entities like the NHS, Dave regularly advises on whistleblowing cases, undeclared conflicts of interest, corruption cases, grievance cases and related personnel issues. Dave lectured for eleven years at the police detective training school in Hendon and has also lectured at other universities and chartered institutions.

Here, Dave shares his expertise in fighting the new wave of fraud in practical terms, based on real-life insights gained from many years of in-field experience.

Table of Contents.

FIRST PRINCIPLE:

Create an Anti-Fraud Culture.

Identifying enabling factors for fraud is the first step towards embedding an anti-fraud culture in your organisation. You can then move on to eliminating these factors with a comprehensive regime of anti-infiltration controls, enhanced vetting, whistleblowing, information technology, and continuous threat-awareness training.

As these are rooted in immutable characteristics of human nature, conditions that invite fraud can exist within any department: human resources, corporate services, and even key technical departments are all equally at risk. Procurement is particularly vulnerable, as are other key functions within finance pertaining to revenue, debt write-off, invoice issuing and receipt, and supplier payments.

In corporate circles, "anti-fraud culture" has had a long run as a catchphrase signifying senior leadership's good intentions about preventing such acts. But no matter how many times leadership repeats the term, the reality of their fraud protections does not conform to their policy statements.

The Association of Certified Fraud Examiners (ACFE) estimates that unaddressed fraud costs the average organisation 5% of its revenue, this number encompasses procurement fraud. The ACFE reports an average loss per case of $1.7 million[4] — not to mention the possibility of untold reputational damage if word gets out. Procurement fraud—often linked to undeclared conflicts of interest, bribery, collusion, or nepotism—has the potential to be one of the largest contributors to the overall fraud figure identified by ACFE.

Whilst speaking, writing about, and investigating fraud for many public and private-sector clients over the course of years, I developed the concept of "fraud-friendly factors" to reframe the issue and break through the complacency of senior leadership. My goal is to reflect on whether their organisation is actually anti-fraud or—in reality—a friendly environment for would-be fraudsters. This perspective has led to an epiphany for many who previously thought the issue was under control.

Fraud-friendly factors abound in a business environment which exhibits:

- Little emphasis on organisational controls
- Abdication of responsibility, as opposed to delegation
- A general laxity towards adherence to the law, one's own corporate standards, and internal regulations
- A trust-based hiring environment, where employees walk in and out with no vetting, no infiltration controls, and no exit interviews to find out why people are really leaving (often at a rate of knots)

"In corporate circles, "anti-fraud culture" has had a long run as a catchphrase signifying senior leadership's good intentions about preventing such acts. But no matter how many times leadership repeats the term, the reality of their fraud protections does not conform to their policy statements."

A fraud-friendly environment is one that is reactive as opposed to proactive. When a fraud is uncovered or whistleblowing occurs in organisations with a fraud-friendly environment, chaos ensues, because there is no pre-prepared plan.

Fraud-friendly means the opposite of planning for the worst but hoping for the best. It means an obsession with the bottom line and with delivering targets, while avoiding warning signs and simply forging forward heedless of risks.

Unfortunately, many careers have ended in fraud-friendly environments. Chief executives, directors, and managers may simply focus on delivery and performance—stripping out layers of control and ignoring segregation of duties. They often won't play ball with internal auditors and try to sweep problems under carpets. They may engage in nepotism and then wonder why the wheels fell off. Or worse still, they end up being duped and sucked into corrupt behaviours because they feel it's simply the way business is done.

That's why I emphasise the concept of fraud-friendly factors and encourage leadership to go beyond catch-phrases and face up to the current state of their culture. Are they running an organisation with a host of fraud-friendly factors in place—whether intentionally or inadvertently? I don't stop asking until I know they're being honest with me—and themselves.

Let's take a closer look at some of the ways fraud-friendly factors play out in real life.

Segregation-of-Duties Erosion.

It would be unwise to rely solely on trust when it comes to providing access to sensitive data and granting authority to authorise procurement spending. An anti-fraud culture must include strong segregation-of-duties controls—the policies and technical restrictions essential in any finance setting to maintain the appropriate authority and access rights required for each role.

However, these restrictions can be eroded over time due to reorganisations, deployment of new systems, streamlining of processes, or routine cost-cutting. Unfortunately, in addition to such unintentional and unnoticed lowering of the protective "walls" separating individual roles' responsibilities and access rights, these controls are often deliberately attacked by persons intent on committing fraud.

Unseen Infiltration.

In the world of fraud investigation, the term "infiltrate" generally refers to an individual working their way into an organisation and a position of trust under false pretences, with a goal of committing fraudulent or criminal acts.

The first step in fighting infiltration often gets skipped when someone is hired for a key procurement role without the proper vetting. This problem may start during the hiring process with something as simple as accepting references sent from a Gmail or Hotmail email account, instead of confirming that references came from the domains of companies where the person claims to have worked. Nepotism can also contribute to the infiltration of bad actors, whether intentionally or not.

Other essential anti-infiltration controls can also be missing from the hiring process, leading to a proliferation of fraud-friendly factors that need to be removed. Though it seems like basic due diligence, many fraud investigations show HR missteps like these during the hiring process:

- Not checking photographic ID to a high standard.
- Not performing essential credit and DBS checking.
- Not doing routine address verification.

In my experience, overlooking such simple but important applicant validation is the first step in allowing a previously unknown individual to walk straight into a company or government agency and perform key procurement operations—often worth millions—for business-critical functions. Such situations can create a high-risk situation leading to fraud, corruption, conflicts of interest, overcharging and invoicing fraud. Remedying the fraud-friendly factor of infiltration due to weak controls during the hiring process is an easy win.

Hesitation about Blowing the Whistle.

One of the most-asked questions at my anti-fraud seminars is about whistleblowing and why it is not invoked properly.

In any business, the informal social oversight provided by co-workers who see wrongdoing and report it to leadership or public authorities can be a valuable check on fraud. When this mechanism breaks down in a corporate culture where staff members are reluctant to share what they know, it creates a rich environment for irregularities to flourish.

Unfortunately, those who have knowledge of crime do not always come forward. The failure of associates to perform such whistleblowing even when they're aware fraud is taking place can result from many factors. But mainly it's due to a lack of awareness of how to do it, combined with little confidence that it will actually make any difference.

Furthermore, some would-be whistleblowers sincerely fear adverse ramifications for themselves if they do report something they consider suspicious—that they themselves might be treated badly as a consequence of raising such concerns.

Worse still, an employee with high integrity who starts to question suspicious procurement processes or decisions will become a fly in the ointment for corrupt managers. These managers may orchestrate overwhelming workloads, unfair treatment, and bullying to break their morale and to cause them to fail and ultimately leave the organisation, which usually happens without any whistleblowing taking place.

And some employees delay blowing the whistle for years, thinking their reports won't be taken seriously because of, for example, their known discontent due to their being passed over for promotion, losing their benefits in a TUPE arrangement, or having reported bullying or harassment by management. So how can you encourage timely whistleblowing, and other fraud prevention steps, by everyone on your staff?

Create an Anti-Fraud Culture.

Clients often ask me what a real anti-fraud culture looks like and how to embed it. I see it first as an environment where hearts, minds, and behaviours are all aligned around a shared set of goals and values. It's an environment where people don't fight against systems and procedures designed to protect against fraud or, even worse, are unaware of them. It's a place where all your team members understand the importance of such controls and apply them to their everyday decisions and duties.

"It will be difficult to embed a real anti-fraud culture without your whole team understanding the importance of fraud prevention and the valuable role they can play in it."

It will be difficult to embed a real anti-fraud culture without your whole team understanding the importance of fraud prevention and the valuable role they can play in it. Similarly, it would be unlikely that a real anti-fraud culture could ever be embedded without conducting a formal counter-fraud risk assessment (which we will explore later) and regular awareness training with every department vulnerable to fraud and corruption.

Training.

To raise awareness of the corporate anti-fraud policy among your organisation's entire workforce, the structured rollout of an engaging training programme is an important first step.

Providing general training on whistleblowing, for example, to the whole staff could be part of a larger programme of organisational ethics training with documentation. This would outline expectations and corporate standards on behaviour relevant to ethics and ask employees to acknowledge that they have read and understood the policy.

In order to make fraud reporting tools accessible, so that employees feel confident to use them when circumstances demand, everyone should know that there are independent staff or officers designated to receive such reports within the organisation—separate from their own line management structure. Most likely, designated staff or officers would include the chief financial officer, head of internal audit, and head of human resources. In some organisations, outsourcing management of whistleblowing is a better option.

In the case of whistleblowing, organisations often fall foul of misunderstanding the rights of whistleblowers in terms of retaining their anonymity and the nature of a protected disclosure generally. You should also provide specialised training for such staff who are designated to receive such reports, so that they are fully equipped to:

- Know their obligations under the Public Interest Disclosure Act.
- Know the rights of a whistleblower.
- Take statements and obtain and preserve evidence properly.

You may consider outsourcing the whistleblowing service to a third-party provider which specialises in receiving and referring such reports, a service which may minimise whistleblower hesitancy in toxic cultures of mistrust and political intrigue.

To remedy a weak or absent whistleblowing service, every company should draft and launch a whistleblowing policy based on best practices developed by fraud-prevention specialists—or review, update, and re-launch their existing policy on the practice.

Making whistleblowing a widely known option in your organisation—along with the documentation and training required to propagate the idea—may seem like a lot of work and an unnecessary expense, but as part of building an anti-fraud culture in your company, it will pay dividends in the long run. According to the ACFE[4], tip-offs are the most common method for detecting occupational fraud. Thus, making this available is advisable.

And making even one person aware of how to securely report possible fraud without fear of reprisal could be worth much more in financial savings, organisational stability, and reputational value than the complete costs of setting up such a programme in the first place.

Accountability

It would be wonderful if every organisation's anti-fraud culture was so pervasive that people in procurement, contracts, finance, and other key roles always did what they should in a secure, legal, and ethical way.

Unfortunately, because people vary in their inclination to do the right thing, an aspect of accountability must be introduced whereby key personnel with responsibility for financial transactions know they are going to be asked about what they're doing to protect the company from infiltration, corruption, bribery, and fraud.

"Building accountability into your team members' daily lives means they are aware that they are always accountable for occurrences of fraud on their watch. They will be aware that if there is a disciplinary hearing or the case goes to court, their career may be over."

Such anti-fraud duties should not only be written into job descriptions but included in a periodic performance appraisal process. Whether such evaluations are carried out monthly, biannually, or annually, key financial personnel need to be judged on their performance in this mission-critical area.

After all, if a staffer has a written obligation to do things in an anti-fraud fashion—to be honest, to have integrity, to spot fraud amongst their staff, to watch for indications of corruption—and this is not formally tasked, they have wiggle room to rationalise that their managers want them to focus solely on outputs, to avoid complaints from customers, and to maximise the revenue stream.

Building accountability into your team members' daily lives means they are aware that they are always accountable for occurrences of fraud on their watch. They will be aware that if there is a disciplinary hearing or the case goes to court, their career may be over.

Once they've created a hostile environment for fraud, organisations should go further, reinforcing that foundation by creating a due diligence culture.

Due diligence culture can be defined as an organisational attitude whereby you know your employees, know our customers, know our suppliers, and know our partners, but it goes much further. The outcome of due diligence should be trust in these parties.

Knowing and Understanding

One person's definition of "knowing" can be very different from another person's definition. To avoid this subjectivity, organisations need to have a clearly defined set of principles and a common understanding.

A notable example is a large government contractor that successfully overhauled its procurement processes, resulting in a significant reduction in fraudulent activities. The company implemented strict ethical guidelines, regular employee training and robust whistleblowing mechanisms. As a result, they reported a 60% decrease in fraud incidents over five years.[5]

SECOND PRINCIPLE:

Create a Due diligence Culture

Due diligence goes beyond knowing your employees, knowing your suppliers, and knowing your partners. It is based on deterring, detecting, and preventing problems before they happen.

1. KNOW YOUR EMPLOYEES:

As described earlier, there are many intentional and inadvertent ways the hiring process can become fraud-friendly. Now let's flip that around and look at how we can avoid infiltration and future potential fraud via a thorough, systematic hiring process.

First, all essential high-risk posts in the organisation should be identified, with all roles on the list made subject to enhanced vetting. In fact, consider outsourcing enhanced vetting for roles identified as high risk (see box).

Potential hires who won't have any purchasing power or the ability to affect procurement could have a more expedited entry into the organisation, with a basic level of checking being sufficient.

However, for staff who could more easily perpetrate fraudulent or corrupt acts, the vetting process must answer the following questions to ensure you know who you're dealing with:

- Are they who they say they are?
- Do their address histories and job histories check out?
- Is there a social media footprint as one would expect?
- Do their references check out properly?
- Will they sign an authority for us to conduct credit checking on them to ensure that their debts are not placing them at undue risk of corrupt acts?
- Would they allow local authority/council checks to be undertaken to confirm whether they're on the electoral register, and whether their council tax is all paid up?
- Will they provide their criminal record check, or will they allow us to conduct this on their behalf?
- Do their identities check out to a high level of scrutiny using independent databases to check the legitimacy of the passport/driving licence they have submitted to us?

HIGH-RISK ROLES FOR ENHANCED VETTING:

- Legal staff.
- Senior HR.
- Key finance.
- Procurement staff.
- Commissioning staff.
- Contract monitoring staff.
- Anti-fraud officers / personnel.
- Physical security staff.
- Corporate management team members.
- Board members.

Another key control in this area is avoiding nepotism. Be careful about employees recruiting family members, close friends, or previous colleagues—the old boys' / girls' network. A simple statement of compliance on applications provides a rudimentary control.

To make sure everything is legal and accurate, all such checking should be conducted by staff trained in essential anti-fraud, anti-corruption, and anti-bribery measures.

Making your hiring process resistant to infiltration by would-be fraudsters is a long-term initiative. Over time, would-be criminals should be significantly deterred from targeting your organisation due to your known good reputation; the robustness of your systems, procedures, and recruitment processes; and your reputation as an organisation that takes direct action and works with law enforcement whenever you find evidence of infiltration, fraud, or corruption.

2. KNOW YOUR SUPPLIERS:

Develop stringent protocols before accepting previously unknown individuals or organisations as suppliers in your procurement system. This includes confirming that a prospective supplier is a real and viable company you want to do business with by:

- Finding out how long they've been in business.
- Validating their references.
- Validating their directors' credibility.
- Checking their credit rating.
- Checking government sanction lists.
- Checking for any known connections between the supplier and employees.
- Checking for reports of environmental, social, and governance (esg) concerns.

And while some of these checks may be performed during supplier selection and onboarding, most organisations perform them only once, or annually[6] — which is far from adequate protection. Supplier checks must be performed regularly, preferably daily. Automated supplier checking is a task that can be outsourced if necessary.

It's also important to keep permanent records of who was involved in recommending or authorising a supplier to come on board. Auditing the names and roles of people involved could provide valuable clues into segregation-of-duties breaches in any future fraud investigation of such a supplier.

SCHOOLHOUSE SCAM

Fraud and a culture of fear.

Sadly, the perpetration of fraud can be found even in the field of education, where I once worked with a large school that had millions of pounds in their budget to provide education to 800 children.

My investigation ultimately revealed that the headteacher had conflicts of interest—joint financial relationships—with a consultant hired to bring in a variety of consultants for the school. Some were allegedly brought in to advise on how best to deal with children with special needs, while others were supposed to help structure finance claims to the local council, and yet others would deliver training to staff.

In the event, interviews showed that no consulting work had occurred in two of the three areas. Sign-in records showed that two alleged consultants were never on site and no reports or email correspondence to or from them showing any work undertaken could be found.

When the school's finance manager was interviewed, they stated they were put under enormous pressure to put the consultants on the system as suppliers and also pressured to process payments to them. They did not blow the whistle because there was a culture of fear in place and people who had raised concerns had simply been made redundant, and their roles "re-organised" out of existence.

Whilst this particular case is currently with the prosecutors to determine suitable criminal action, the headteacher was disciplined and dismissed for gross misconduct. An application has also been made to the governing body for head teachers and teachers in the UK to disbar this individual from being able to access similar roles in the future.

3. KNOW YOUR BUSINESS PARTNERS:

Companies and individuals may approach you out of the blue with opportunities for collaboration, investments, or joint ventures. But it's essential to perform due diligence on any prospective business partners who approach you by asking the following questions:

- Does the person approaching you actually link back to the company they purport to be from? Simple open-source checking can help with this, as well as asking for their landline and extension number and checking the email addresses to make sure they match to the stated company's URL. It's remarkable how many people never perform even this simple level of validation.
- If they do connect to the organisation they say they are from, is this a legitimate business? Is it registered at Companies House? How long have they been a business? Who are the directors? What did the last set of accounts show in terms of profitability?
- Do their trade references actually check out? You should not have any discussions or do any business until such references have been sought and received, and a site visit undertaken.

Four types of references are normally essential: professional references, personal references, bank references and customer references - often from reference-service websites that will provide a testimonial. Specialist companies, private investigators and corporate fraud investigators can all assist in conducting independent due diligence checks on any prospective business partner or those seeking investment and will check each of these four types of reference.

In addition to the factors outlined above, the following guidelines will help ensure that a comprehensive due-diligence ethos gets embedded in your organisation's culture.

Enforce and Review Conflict of Interest Checks.

When essential procurement projects take place—particularly at the tendering stage—potential conflicts of interest need to be declared in writing by procurement-panel members and key decision-makers. The problem I have seen is that either these checks are not conducted; an uncompleted form is signed and submitted, or people simply do not declare their real conflicts of interest. Even more worryingly, people may declare their conflict of interest, but the form is simply put on file and no one takes any action or does any further checks.

If such requests for complete and accurate documentation are not taken seriously—and no disciplinary action is taken for noncompliance—there is a definite risk that this check comes to be seen as simply as a rubber-stamping exercise.

Use Open-Source Information to Review Relationships.

Related to the previous point, a lot of information can be sought through simple online searches, revealing a raft of different relationships which have not been declared previously.

For example, Companies House can show who among your employees is or was a director at various companies in the past, and therefore have a potential conflict of interest that was not declared.

Similarly, previous employment can be found on LinkedIn, revealing relationships to current suppliers or staff members.

Ensure Suppliers Have Their Own Anti-Fraud Controls.

Since partner organisations might want to corrupt your own procurement and finance staff, it's important during the tendering process to demand that your key partners share your ethical ideals, with anti-fraud and anti-corruption controls embedded in their own organisations.

When a tender is put out, one essential pre-qualification question should centre around the bidder's ethics and probity standards. For example:

- Do they have any European, British, or other national accreditations pertaining to anti-fraud and anti-corruption?
- Do they have their own internal policies and regulations and training pertaining to anti-fraud and anti-corruption?

"The best prevention, deterrence, and detection strategies come from embedding best practices identified in a formal counter-fraud assessment process."

Questions can also be asked about the amount of investigations/whistleblowing they have had and what the outcomes were: will they agree to an open-book financial policy with you so you can scrutinise their records if needed? Will they work with you if investigations necessitate joint effort?

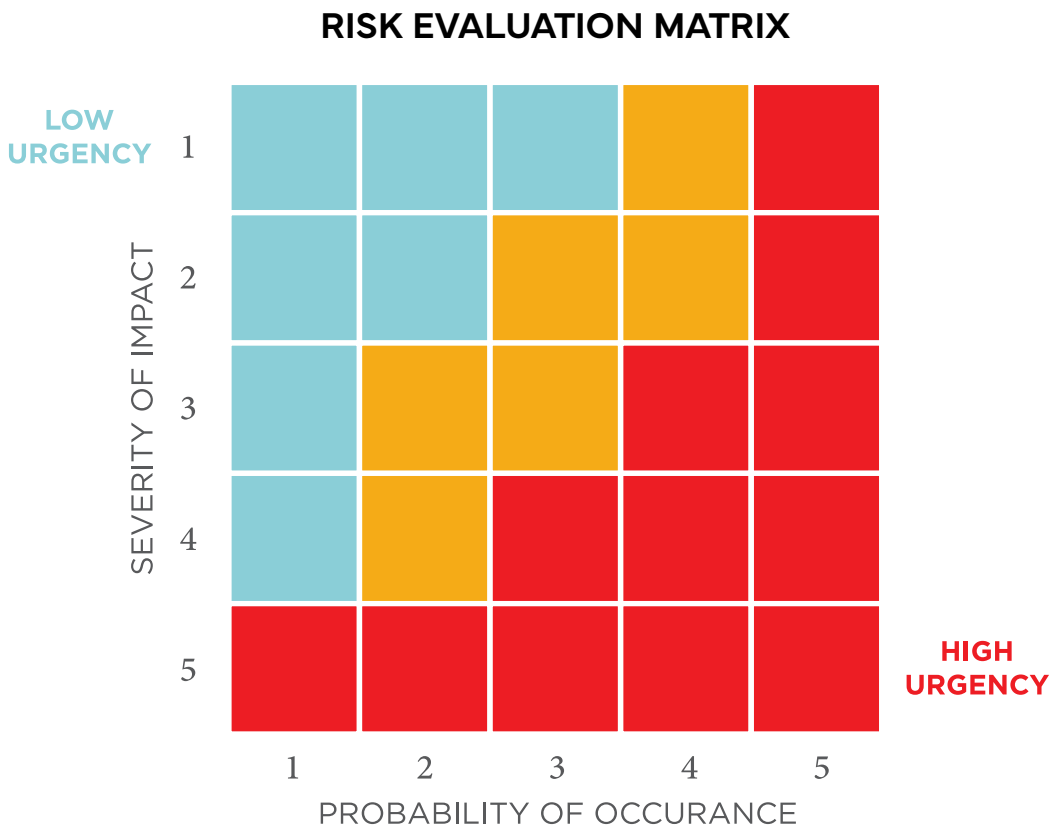
You can also ask questions to judge their general professionalism in terms of security pertaining to data protection requirement adherence, anti-money laundering policies, and information security best practice.

Evaluate Risks Regularly.

The best prevention, deterrence, and detection strategies come from embedding best practices identified in a formal counter-fraud assessment process. This should be a continuous cycle, done formally on an annual basis but updated regularly as new threats unfold, incidents occur, and new risks come to light.

The essence of the counter-fraud risk assessment process is to evaluate the impact and likelihood of various fraud risks. This is done by meticulously listing all departmental functions and evaluating them accordingly.

Though it may be helpful to bring in an expert on this methodology the first time you do it, the conceptual foundations of the exercise are simple: it starts with listing the risks to the departmental functions referred to earlier and then scoring each on a scale of 1 - 5 for likelihood and 1 - 5 for impact. By multiplying the two scores, you can determine the relative urgency of mitigating each one.



The organisation then has various options to mitigate the risk, based on their risk appetite and whether they wish to terminate, tolerate, treat, or transfer the risk. Most organisations seek to treat risks by implementing appropriate controls.

THIRD PRINCIPLE:

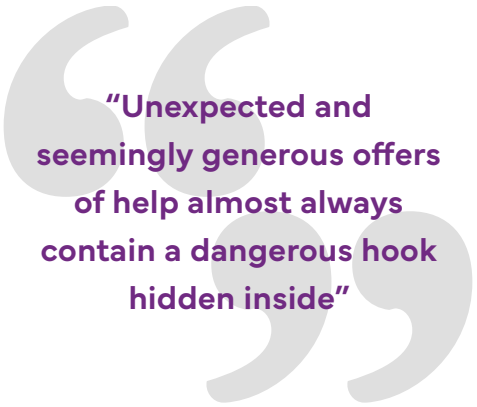
Defend Against Social Engineering

The biggest vector for an infection of fraud is not technology—it is the vulnerability of your employees to criminals who play on normal human emotions.

What is social engineering? Essentially, it is how criminals gather information about their intended victim and use coercion and confidence tricks to get them to do something they would not have ordinarily done, often by impersonating another person or company.

In the world of corporate fraud, and procurement fraud in particular, social engineering is used as a method to infiltrate, gain the confidence and trust of key staff, and ultimately gain access to confidential information that allows fraudsters to receive an illegitimate payment by passing themselves off as someone else.

The goal may also be to unfairly gain market advantage by acquiring confidential commercial information about a procurement project. This can take the form of an employee tipping off a friend outside the company about a bidding opportunity before it is open for public bids, in contravention of company guidelines or regulatory policies. It can lead to under-bidding in an effort to eliminate competition, followed by overcharging in a now less-competitive market. Sometimes undetected cartels engage in coordinated over-bidding to fix prices and thereby control the market, forcing all purchasers to pay more and get less.



Fraudsters often find that the best way to socially engineer your staff is to compliment them, befriend them, ascertain their financial and/or personal problems, and then offer them work, better prospects, favours, holidays, or cash. This may be sufficient inducement, but if not, evidence of these bribes can be used as blackmail to achieve the fraudster's goal.

To become convincing, fraudsters frequently use social engineering techniques to piece together information about the person they aim to impersonate. They use public sources of information and "phishing"—for example, calling a company and asking to confirm the email address of the target they are supposedly having difficulty with (when, in fact, they don't have the email address at all), providing one more clue which can then be used in the deception.

Criminals can come across as being empathic, sympathetic, complimentary and understanding. But the seemingly generous offers of help that follow always contain a dangerous hidden hook inside, potentially leading their victims to unexpected depths of bribery and corruption.

Social Engineering and Procurement Fraud.

The key risk stages in procurement fraud are at the pre-procurement phase, the delivery phase, and the post-procurement phase. In other words, criminals seek to socially engineer your employees at every stage!

For example, they may seek to gain confidential information in the pre-tender stage and to develop conflicts of interest. They can then use those conflicts of interest in the delivery stage to sign off substandard work, over-inflate invoices, or to cover for double invoicing in the post-procurement stage. Indeed, procurement fraud rarely operates without invoicing fraud, in terms of over invoicing, duplicate invoicing, or false invoicing.

Conflicts of Interest in a Procurement Setting.

Senior staff, procurement staff, directors, and those responsible for budgets and contracts are typically hired for their experience, skills, and record of success. You assume they've earned the trust and confidence placed in them and have the best interests of their employer at heart, rather than feathering their own nests or the nests of those close to them. But they're also human, and being placed in responsible positions naturally opens them up to potential conflicts of interest.

Conflicts of interest can be extremely covert: imagine a director approaching a junior staff member diligently revising a spreadsheet and asking them to mark the tenders received in accordance with a new marking scheme. Putting emotional pressure on them to be lenient in some regard, or to mark the tender in a way that is inaccurate, may be intended to favour the company with which the director has a relationship.

Other conflicts of interest are simply based on inertia and tradition: purchasing often occurs without a formal tendering process and historical or preferred suppliers are simply retained for security work, CCTV installations, cleaning, staff canteens, IT infrastructure, consultancy work, repairs, routine maintenance, fleet provisioning, and materials and machines.

Conflicts of interest like these may not have been pre-existing but have been nurtured by the supplier during many years of working relationship.

Of course, your key personnel may have family and friends outside of the organisation who could be prospective suppliers. Such individuals and companies may do a splendid job and have as much right to a contract as anyone else if the relationship is fully disclosed and they bid in a fair process (with boundaries placed around the actions of key decision-makers). But you could also get shoddy work if your staff is sharing secret information that gives such suppliers an edge over more economical or better-qualified competitors.

There can also be a serial problem of contract variations, whereby even if the corrupt parties were brought in to deliver something cheaper and better, they turn out to be far more expensive in the long run due to high levels of contract variation—signed off fraudulently—once they get their feet under the table.

Other conflicts of interest can arise through gifts like a bottle of alcohol at Christmas, but it's more likely to include meetings held in expensive sporting venues and the provision of lavish entertainment. This type of corruption can quickly spiral out of control with monetary "inducements" which are, in fact, bribes.

Conflicts of interest are easy to spot by imagining a few simple questions: in the public sector, what would a behaviour look like if it was published in the local newspaper or national media? For example, how would the story look if a senior official in the Department of Health gave a critical PPE contract to their brother-in-law's company?

In the private sector, how would shareholders view the actions? For example, if it was exposed that a national company had been procuring its IT infrastructure through a company owned by a director's wife at inflated rates, and an investigation revealed millions of pounds worth of overcharging and under-delivery, how would shareholders react?

FOURTH PRINCIPLE:

Leverage Information Technology

Artificial intelligence (AI) technologies such as machine learning, deep learning and natural language processing can detect unusual patterns, even in high-volume procurement workloads, with speed and accuracy that no human can match—offering far better detection of anomalies than random samples or manual audits.

Today's workflow within the cycle of procurement, invoice processing, and supplier payments is built almost wholly on information technology, using software that now often runs in the cloud. This transition from manual, paper-based processing to online and automated processing was once optimistically envisioned as the glorious final frontier for efficiency, security, and consistency.

Recent advancements in AI and machine learning have revolutionised fraud detection. AI tools can now analyse vast amounts of transaction data in real-time, identifying unusual patterns and anomalies with unprecedented accuracy. Machine learning models continuously improve by learning from new data, which enhances their ability to detect fraud. Companies like Kroll have highlighted the critical role of AI in anti-money laundering (AML) and other financial crime prevention efforts, emphasising its effectiveness in improving compliance and reducing the risk of fraud.

One advantage of AI is that it continues to improve—finding new patterns and exceptions that it "thinks" might be of interest and getting more accurate in its identification of risks. This significantly improves the protection AI provides. Plus, AI is fast and examines all available data. It's not merely sampling, as with most audits, and as a result it doesn't miss anything like humans inevitably do.

Unfortunately, new factors have emerged that have changed many organisations' risk profiles in the procure-to-pay cycle:

- As technology continually evolves, procurement and finance systems are often being replaced, upgraded, or migrated to the cloud, making it challenging for staff to keep up with changes in how to secure these applications from fraud risks.
- As staff alternate between working remotely and returning to the office, system permissions may have to be modified and access from outside networks reconfigured, leading to potential security gaps.
- With HR challenges and budget constraints—along with assumptions about automation's actual impact on staffing—fewer staff are being asked to do more, possibly leading to corners being cut and processes not being followed.
- Suppliers are moving to eProcurement and eInvoicing systems to remove paper and PDF documents —a transition being mandated by governments around the world, often as a way to improve tax reporting.
- Hackers and fraudsters are finding and exploiting new weaknesses in systems and processes.

As a result, established and relied-upon controls have become out of date. The risk landscape has changed, with new systems and working arrangements bringing new risk entry points that can be exploited if they're not properly identified and mitigated.

Case Study

A global financial services firm integrated AI-based detection tools to monitor transactions in real-time. This proactive approach enabled them to identify and prevent a major procurement fraud scheme involving false invoicing, saving the company approximately $2 million within the first year of implementation.[7]

TOOLS FOR A ROBUST PROCUREMENT PROCESS

Procurement professionals do not work alone in their quest to establish and maintain robust procurement processes. Best practices are enshrined by the Chartered Institute for Procurement and Supply[8], an organisation which offers training and resources for personnel in this field. UK organisations dealing with public sector entities can also turn to PCR, the Public Contracts Regulations, and there are various European procurement laws which need to be followed, depending on the material value of the contract being tendered.

In procurement, information technology is not only the foundation for automation-assisted bidding and payment processes—It can be a valuable tool for tracking the integrity of procurement processes. One example of a key control for meeting this goal is using a "write-only" procurement portal. This technology ensures that contracts are advertised through the portal, that tenders come in through the portal, that any questions asked are all monitored and responded to through the portal, and that any actions outside of this process can be deemed to be nefarious and subject to disciplinary action.

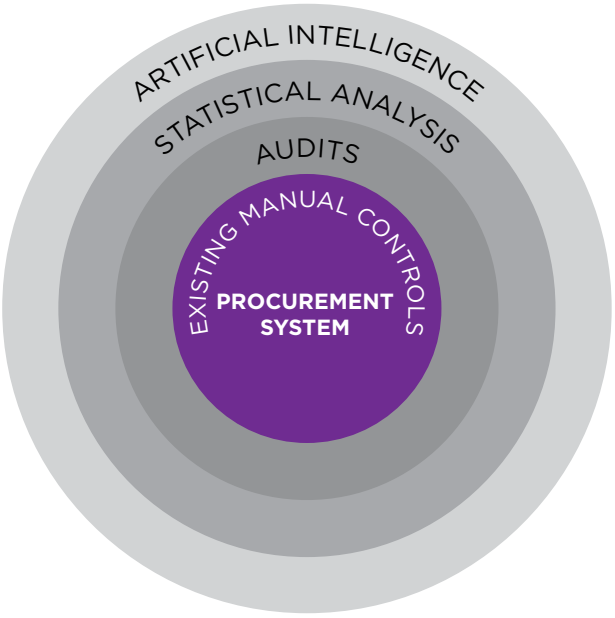
Multi-Layer Protection.

Anti-fraud controls have been deployed within existing IT systems over many years, but they are generally manual or require significant manual input. Technology provides the opportunity to add to these controls by offering new, fully automated checks and exception alerting, as well as automating some of the previously manual tasks.

Additional controls are needed to augment existing fraud protection measures. A multi-layered approach gives the best protection.

Organisations should continue to utilise any fraud-detection functionality built into their existing procurement systems and processes, where viable. These form a useful first layer of protection against fraud.

MULTI LAYER APPROACH FOR 100% PROTECTION



But based on the new confounding risk factors outlined above, organisations also need to look for exceptions and anomalies that indicate previously unseen causes for concern and add appropriate detection and prevention control mechanisms.

A combination of AI and established statistical analysis available in mainstream procurement software works best. For the highest level of protection, search for a solution with multiple AI methods and non-AI methods that work together.

FIFTH PRINCIPLE:

Investigate and Assess

Investigate fraud and work on prevention via ongoing proactive anti-fraud checks and assessments.

Proactive Versus Reactive.

When looking for past payment irregularities, there is a tendency to rely on procurement and accounts payable audits to find historical issues. This used to be the only way to operate due to the effort required to comb through data, searching for anomalies. In accounting, this is still the prevalent mode of thought: take steps to avoid mistakes, but—if they do occur—the next audit will pick them up.

This has always been a necessary and reasonable approach, since the effort to manually check all transactions in sufficient detail was way too high and the speed of doing so prohibitively slow. Hence sampling was introduced to audit a random selection of transactions—often only those above a certain monetary threshold.

Such constraints make auditing unsuitable for providing a high level of protection. Not everything is checked, and audits are—by their nature—post-event. And fraudsters know how to exploit loopholes like monetary thresholds.

But advances in technology and the cost reduction of compute-intensive applications like AI have removed the need for audits to be infrequent and to rely on sampling. Further, due to the speed and frequency with which AI, statistical analysis, and other pattern matching techniques can now be applied to the task, risk detection can move from reactive to proactive.

"Optimum results are achieved with automated preventative analysis and risk detection running continuously in the background"

In most organisations, a daily check of all procurement, purchasing, and accounts payable activity over the last 24 hours using a multi-layer approach would provide a highly efficient and preventative approach.

Such technology reduces procurement fraud risk by analysing supplier record updates and invoices before the next purchase order is sent to the same supplier. By analysing transactions as soon as they are entered into the accounting system, the proactive approach allows exceptions to be flagged quickly enough to put a suspicious transaction on hold before the supplier is paid for a potentially fraudulent transaction, or a bogus supplier is paid for a legitimate transaction.

Optimum results are achieved with automated preventative analysis and risk detection running continuously in the background. The proactive system's interface is capable of breaking into users' workflow when a potential fraud or other risk type is detected. Users are shown why it's considered a high risk that needs attention, giving the operator the chance to investigate and resolve the issue before any significant damage is done.

Proactive Conflict-of-Interest Checks.

The tried and tested method to avoid potential conflicts of interest is to proactively do checks consisting of enhanced vetting at the recruitment stage, and ongoing checks—at least annually—for those members of staff where the counter-fraud risk assessment indicates they are at high risk of conflicts of interest, bribery and corruption. The staff normally includes your internal auditors, counter fraud staff, procurement staff, legal staff, finance staff, commissioning staff and contract managers.

Spend Analysis.

Spend analysis is often deprioritised because of heavy workloads and the urgency of day-to-day operations. The resulting lack of spending insight can cause a significant fraud risk. Procurement managers are often busy with team deliverables, dealing with problems, and other day-to-day challenges. Finance managers are normally busy ensuring Accounts Payable and Accounts Receivable operate efficiently. Conducting fraud-oriented spend analysis can be a very telling exercise to detect potential overbilling, suspicious suppliers and payments, and conflicts of interest.

Forensic Procurement Audits.

Like spend analysis, forensic procurement audits are something that rarely occur in most organisations. This is where tenders are analysed at a forensic level to see if a real competitive process was actually undertaken. For example: who oversaw the tendering process? What portal was used for communications with would-be suppliers? Was there segregation of duties between the various functions involved?

There are many other points to consider during a proactive forensic procurement audit, which a qualified professional fraud expert can work through with you. This may include analysing communications between the commissioners and would-be suppliers, including email correspondence, giving particular scrutiny to any challenges to the procurement process and the associated responses sent.

"To increase protection from all types of procurement fraud, public and private sector organisations should conduct an annual counter-fraud risk assessment"

Structured Counter-Fraud Risk Assessment.

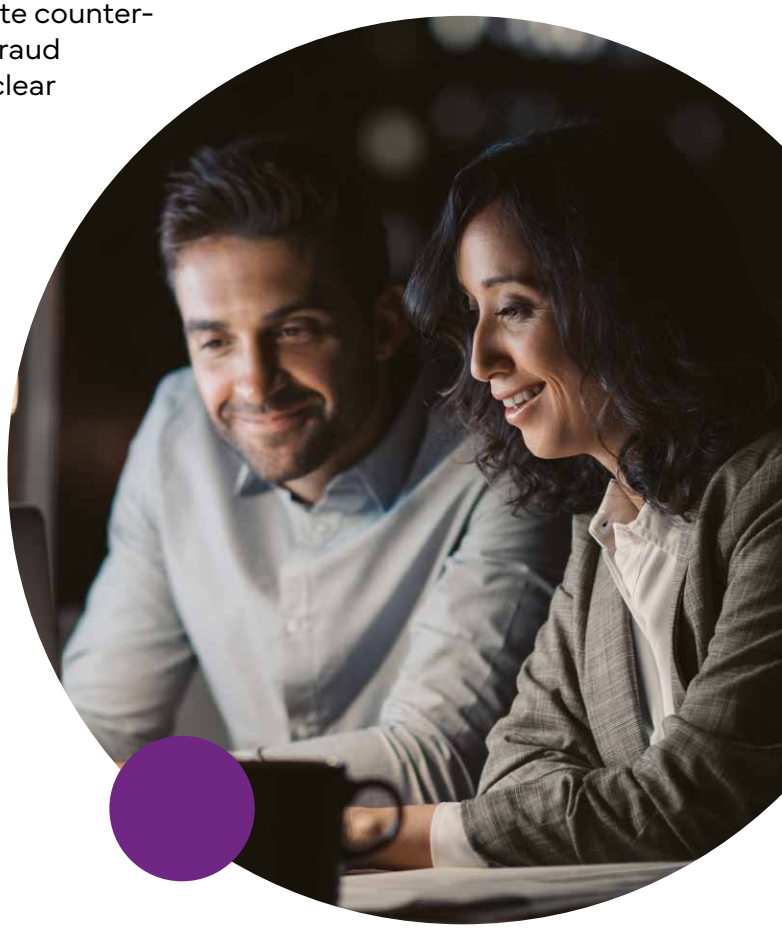
The counter-fraud risk assessment is a structured process in which controls, processes, fraud response plans, proactive audits, and compliance checks are all listed and reviewed.

Ideally, the entire corporate entity should undergo an annual counter-fraud risk assessment—department by department and area by area, with individual key procurement projects also entered into the assessment. Alternatively, if an organisation is not at the stage of maturity to have an overarching approach to procurement fraud prevention, the counter-fraud risk assessment might just be done on a particular high-risk procurement project.

The first document generated in this process is an overarching annual corporate counter-fraud risk assessment report. This report explains the methodology, conclusions, findings and key recommendations pertaining to the entity-wide counter-fraud risk assessment being undertaken. The document would contain appendices organised department by department and area by area, showing a line-by-line evaluation of risks, scored in green, amber, and red to visually flag various items and areas by their risk level.

When completed, the corporate counter-fraud risk assessment would be entered into the organisation's complete risk register. This file of documents typically also holds the risk plans pertaining to physical security, health and safety, pandemic response, disaster response, information security risks, information security disaster response, and any other pertinent risk plans drawn up by the organisation.

Unfortunately, it is inevitable that certain fraud risks will likely materialise regardless of our attempts to prevent and deter them; for example, business email compromise and bank-mandate fraud attacks are relatively new types of risk. So, a key addendum to the corporate counter-fraud risk assessment would be the "corporate fraud response plan." This document encompasses a clear plan of actions, responsibilities, accountabilities, documents, and time scales to help the organisation respond to any and all fraud attacks when they are discovered.



Conclusion and Recommendations.

I created this document with the goal of providing both high-level knowledge and detailed action steps to empower senior leaders within organisations vulnerable to procurement fraud—which could be just about any organisation that has staff performing dedicated contracting, procurement, and accounts payable functions. I hope this information will empower executives to have informed conversations about fraud prevention with their peers, or those with procurement and finance related responsibilities who report to them.

Given the evolving nature of fraud threats, organisations must adopt a dynamic approach to fraud prevention. Key recommendations include:

- Invest in Technology: Prioritise investments in AI and machine learning to enhance fraud detection capabilities.
- Strengthen Internal Controls: Implement robust internal controls and regular audits to identify and address vulnerabilities.
- Foster an Anti-Fraud and Due Diligence Culture: Encourage ethical behaviour through continuous training and transparent reporting mechanisms, and defend against social engineering.
- Conduct Proactive Risk Assessments: Regularly perform risk assessments to identify emerging threats and adjust strategies accordingly.

Sometimes the best way to begin taking action toward a desired goal is to ask questions and see what the answers tell you about your current status and required progress. To that end, I suggest that the following personnel in your organisation work through the example questions listed, as a basis for assessing your anti-fraud readiness and fulfilling your responsibilities to the chief executive and the board:

HUMAN RESOURCES DIRECTOR:

- What sort of anti-infiltration controls do we have?
- Do we have an enhanced vetting procedure for applicants to high-risk roles?
- What do we do to ensure whistleblowing occurs and the staff feel confident to come forward?
- How do we support the disciplinary process if investigators find fraud or corruption?
- How do we avoid the compromise agreement culture?
- How do we avoid ending up in employment tribunals, making compensatory payments to potential wrongdoers because we did not follow proper protocols and legal procedures?

FINANCE DIRECTOR

- What are the key at-risk areas within the finance function, in your opinion? (Break out risks on the income side, the expenditure side, the payroll side, and the expenses side.)
- What are we doing to avoid bank-mandate fraud?
- Who are our top suppliers? Are their invoices all in order? Do we reconcile statements and payments?
- Is there a suitable audit trail on our finance systems?
- Do we use any specialised technology to spot fraudulent transactions?
- Are we proactive as a finance department in the fight against fraud, or are we reactive?

PROCUREMENT DIRECTOR

- What are we doing to prevent, deter, detect and investigate procurement fraud?
- What do our staff do on a daily basis to prevent, deter and detect procurement fraud? Where do we think the main risks reside: the pre-procurement phase, the delivery phase, or the post-procurement phase?
- Are suppliers continuously validated?
- What do we do to work proactively with our finance department, HR department, and investigators to prevent and detect procurement fraud?

HEAD OF CORPORATE GOVERNANCE

- What systems and regulations do we have in place to prevent fraud and corruption?
- Do all whistleblowing procedures get used?
- What were our last three big cases that came through whistleblowing? Were they investigated? What was the outcome?

HEAD OF AUDIT AND INVESTIGATIONS

- Do you have adequate resources trained and available to react to procurement fraud should it occur?
- Are your investigators aware of this type of fraud?
- Do you run proactive forensic procurement audits?

About FISCAL Technologies.

FISCAL Technologies provides forensic AI-powered software and services that empower progressive Procure-to-Pay, Accounts Payable and Shared Service Centre teams across the globe to protect organisational spend and eliminate supplier risk.

Our award-winning, cloud-based software uses forensics and AI to provide a unique view of risk. It's used to find duplicate payments, defend against fraud, automate manual processes such as statement reconciliation, help optimise working capital and provide trusted reports.

Since 2007, leading private and public sector businesses have trusted us with guarding £300 billion in spend - the equivalent of 15% UK GDP. On average we save each customer of £258 thousand per year.

About The Author, Dave Verma MSc, Principal Consultant.

I help private and public sector clients in confidential, complex, and often contentious fraud investigations (and any other type of investigation).

I work with my clients to establish whether there is a case to investigate, coordinate the different phases of the investigation and assign responsibilities to and develop timelines with specialised auditors, investigators and other personnel. I also help undertake interviews of whistleblowers, witnesses, and suspected perpetrators within the workplace.

On the proactive side, I like to help organisations with training and awareness and conduct counter-fraud risk assessments to give clients a more informed view of the risks they actually face and how to address them.

Sources.

1. https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html
2. Procurement Fraud Statistics 2024 — 20 Key Figures https://procurementtactics.com/procurement-fraud-statistics/
3. https://www.extrapolate.com/information-technology-communication-iot/fraud-detection-and-prevention-market/21586
4. ACFE 2024 Report to the Nations https://legacy.acfe.com/report-to-the-nations/2024/
5. https://www.bradley.com/insights/publications/2024/02/procurement-fraudrecoveries-substantial-for-doj-in-fy-2023
6. Purchase to Pay Network 2022 survey report https://fiscaltec.com/resource/ppn-supplier-risk-management-report/
7. https://procurementtactics.com/procurement-fraud-statistics/
8. https://www.kroll.com/en/insights/publications/fraudand-financial-crime-report

t: +44 (0) 845 680 1905
e: smarter@fiscaltec.com
w: www.fiscaltec.com

Document ID: Principles of Procurement Fraud Prevention 2024 06