Corruption and the Insider Threat

Global Risk Alliance Ltd

The Insider Threat: Testing the effectiveness of your fraud controls, are you doing the basics?

Do you focus on identifying high value fraud and ignore the risk of high volume low value fraud? An insight into why an assessment of the risk from regular low value contract fraud is important.

> A good decision is based on knowledge and not numbers.
>
> — Plato

A case prosecuted in Canada highlighted a number of key issues surrounding the insider threat and the organised network that was developed to undermine the compliance controls and give the impression of competition within the procurement process.

The Chronicle Herald reported that a judge found a private contractor and a civilian employee guilty of defrauding the federal government in a scheme related to a heating plant.

An employee responsible for procurement for the Air Force base's massive heating plant was found guilty in plotting with his friend and businessman, to direct contracts to four companies owned by the latter. It was alleged that over a four year period the three men involved defrauded the federal government of over $2 Million.

Methodology

Four companies were created to give the impression of competition in the tender process, specifically to provide the number of bids that were required to seek for contracts under $5,000. What isn't clear is whether the work was carried out. It also means if the maths is correct that in a four-year period there was a minimum of four hundred low value contracts awarded to these companies.

Insider knowledge

In this case the procurement professional knew the financial thresholds and that anything over this amount would have required additional scrutiny and approvals.

What is missed in many organisations is the scrutiny and data analysis of low value procurement because there can be a perception that there will be no fraud or if it's a low value contract then any fraud will be minimal and hardly worth wasting any time on. However, when they are low value and regularly awarded they soon mount up to high value fraud.

Control measures are put in place for the high value procurement because there may be an increased risk of fraud or financial risk. I have also seen cases within international organisations where allegations under a specific value will not be scrutinised due to the number and cost of cases under investigation.

Control measures

The full facts aren't clear just from a press article, however one of my first questions is always, how did they get in the front door. The control safeguards at the vendor onboarding failed. How did four companies owned by the same individual pass screening that should have included verifying:

- the date of company formation against vendor registration date
- company directors and shareholders checked against staff and supplier data for conflicts of interest
- supplier visits to confirm the establishment and size of the business
- ability to perform contract if they were a brand new company

Additionally, as part of procurement data analysis there should be checks carried out to look at values around the tender threshold levels to determine whether there is irregularity and avoidance of additional oversight and financial management.

It isn't uncommon for staff to split orders to keep them under the threshold for a number of reasons, that might include the perceived additional bureaucracy or delays that might be incurred when introducing a tender process. It doesn't mean that it's corrupt it may simply be a breach in procedure. Root cause analysis in these cases including documented decision making and approvals needs to be established.

The ability to verify work is finished should also be in place including segregation of duties, specifically the person ordering the work shouldn't be the person verifying the work has been completed.

The insider knowledge that the vetting system was weak that allowed for the registration of ghost companies and the manipulation and rigging of the procurement route. The implementation of vetting and procurement procedures would have brought this scheme to light much earlier and may have stopped it before it had chance to begin.

The Hidden Threat: Manipulation and Abuse of Payment Control Measures.

Do you have adequate financial control measures; Do you test your payment system for an insider threat. It is the insider that recognises the compliance weaknesses in organisation procedures and the gaps in control measures, so do you use trust as a control measure, and are you willing to take the risk that your staff won't defraud your organisation?

> Beware the allure of shortcuts; they often lead straight into the arms of procurement fraud.
>
> — Global Risk Alliance Ltd

There are many ways in which an illicit payment can be hidden. Procurement corruption can take many forms where it has been agreed to facilitate the award of a contract, the bribe payment can happen before or at the time of award, can be given from the profits during the lifetime of the contract, that can include an agreed percentage of the contract value.

Urgent requirements

Do you consider how to prevent corruption in procurement?

In organisations where there are regular urgent requirements or short deadlines for goods, works or services to be provided it can become much easier for individuals to request a bribe. There is always pressure on an organisation in order to speed up the process to relax procurement controls and introduce direct award contracts rather than tender.

Individuals within an organisation that can influence the procurement process will always know where the gaps are in the controls regime and how to exploit them. Fraud and corruption become much easier where there is no documented contact with suppliers or new vendors, where there can be a lack of visibility of individuals contact, communication and relationship and an environment can be created where an individual's corrupt behaviour is hidden. Due to the lack to documentation, where allegations are made about this behaviour there is likely limited ability to verify these suspicions or allegations.

Advanced payments

In some regions globally, it appears to have become more common to use advanced payments for suppliers to expedite urgent requirements, that can on average amount to between 50 to 100 percent of the contract value. However, it has been noted that in many cases the procurement isn’t urgent, and it has become custom and practice to use this method of payment with certain suppliers.

Where this method of procurement and payment is common there is an increased risk that a bribe payment could be requested, specifically incorporated into the advanced payment and handed out as cash by the supplier. It also makes it easier for fictitious requirements to be created and payments diverted or for suppliers to make off with the payment without providing goods, works or services.

The illicit payment in many cases is hidden because of the procurement route used, the lack of information generated, and the method in which the payment is made. This is particularly relevant where there is no consistent approach in the verification of completed works or services and that quality standards or specifications have been met?

Organisations that have a high volume of procurement and invoicing and have limited staff to manage these outputs can create a situation where checks and balances are missed or not carried out because of excessive workload.

As an example, at first glance it may look like individuals in finance who administer such payments may be involved, but may, where there is an excessive workload or pressure to approve payments may hinder thorough scrutiny of invoices and supporting paperwork.

Change of bank account details

There are many justifiable reasons why a supplier would change their bank account, that might include something as simple as bad service from a provider. Organisation's when assessing the risk within financial systems, regardless of the dual controls in place to change bank account information should annually assess the volume of these changes and use a data analysis approach to determine whether these changes were legitimate or to corruptly divert funds.

Examples of this type of illicit activity in the diversion of funds might include:

- Numerous suppliers and their payment being diverted into the same account
- Changing an account to a different country account and company name
- Using a different language to describe the company name
- The company name and the name of the bank account are different
- Payment that have no bank account information on the finance system

Control measures

A very simple bribery and financial crime method, however, this risk can be mitigated by the introduction of procurement and finance control measures and a risk management and compliance approach, specifically:

- Does your organisation have a published procurement policy outlining single source and urgent requirement procedure?
- Do the procedures define the circumstances in which advance payments can be used?
- Does your organisation have a single source justification procedure?
- Are these procedures followed and it non compliance data retained?
- Use proactive data analysis to verify which companies regularly receive advanced payments. Are they justified or is there a pattern of non compliance with the policy?
- Are these procedures audited for non compliance?
- Do you conduct consistent data analysis on finance and procurement systems?

Conclusion

Although an organisation should have ethics and anti-bribery and corruption policies and procedures including a hotline that will allow suppliers the opportunity to report a bribe request, it is only when you introduce and follow procurement and finance policy and procedures that you have a greater opportunity to mitigate bribery risk and introduce a more robust compliance programme.

Does your leadership recognise the benefit of having trained procurement professionals, that the management and compliance with finance procedures can never be underestimated to protect the revenues of an organisation. Do you think that introducing procurement procedures to make things simple or speedier will have a negative impact on your organisations bottom line.

Procurement Transformation: How To Identify And Reduce Your Corruption Risk.

Where would you start? If you are ever put in the position of creating an assessment of whether your organisation has adequate corruption and procurement fraud risk mitigation in place, after taking a deep breath, an initial focus should be on planning a risk assessment of your organisation's procurement lifecycle and compliance capability.

> Quality means doing it right when no one is looking.
>
> — Henry Ford

There is no one size fits all approach to evaluating the external and insider threats that an organisation can face from corruption and procurement fraud including the mitigation procedures that should be put in place to counter these risks.

Such an assessment shouldn't be a tick box approach of common risks or control measures that have been researched online but designed around the assessment of an organisation's current anti-corruption approach and framework to help identify the gaps in current control measures to procurement fraud and corruption risks identified within the risk assessment.

There are many areas to consider in an assessment approach that includes during vendor onboarding, manipulation of procurement route, pre and post award procurement stages, contract management, and the end of life and disposal of assets.

A walk through of processes and compliance programmes with the relevant organisation expertise including finance, procurement, security, projects, quality assurance, and projects will further identify risks from different perspectives.

When evaluating risk mitigation requirements, an assessment should first be conducted to determine which are the key risk areas. This will ensure that an organisation can properly task and coordinate its finite resources.

Part of the problem in assessing risk is the availability or access to internal information sources including limited knowledge in identification of relevant data sources that are of value to the assessment, which in itself can be a significant risk where assessments are being made resulting in an incomplete risk picture.

Many organisations have departments that protect their own data and don't share it with other departments including compliance, which can create a situation where the scale of a problem is underestimated or unknown.

Case study

A case example includes an investigation surrounding an insider threat and the improper award of single source consultancy contracts. The conclusion of the investigation confirmed that an individual within a project team who received early notice of the initial consultancy requirements had set up his own recruitment company to identify consultants for these requirements and facilitate the award of consultancy contracts through his own recruitment company.

What later became clear was that an audit of the organisation's single source procurement procedures had been conducted at the same time as the investigation without the knowledge of the investigation team. The conclusions of the audit raised significant concerns surrounding the gaps in the justification and authorisation process including the control failures in a significant number of single source contracts.

The disconnect between departments within the same organisation meant that if this information had been shared with the investigation team at the time, then they might have better understood the scale of the risk and had the opportunity to assess whether other cases or individuals were involved.

Risk mitigation framework

To determine whether your organisation has the ability to assess and mitigate its own risk, a number of initial questions should be answered:

- Do you have a communication strategy to build organisation culture and respond to corruption and procurement fraud risk?
- Do you have a corruption and procurement fraud response plan?
- Do you have documented investigation procedures?
- Have you conducted a project assessment for corruption and procurement fraud risk?
- Have you assessed your organisation's capability against BS10501 British Standard, Guide to Implementing Procurement Fraud Controls, and ISO37001: Anti-Bribery Management Systems?
- Do you have a structured training programme that outlines current corruption and procurement fraud risk, impact and risk mitigation?
- Can your organisation centrally collect and analyse its own data for corruption and procurement fraud risk?
- Do you conduct an annual assessment of your procurement lifecycle for corruption and procurement fraud risk?
- Is there asset tracking as part of your organisation's asset management procedures?
- Do you have asset disposal procedures for goods and materials that are obsolete, scrap, damaged or write-offs?

What will your approach be

The answers to these initial questions will give you an insight into whether your organisation has the ability to assess its risk and if it can adequately respond to it. If you are unable to answer these questions fully, then you may want to ask yourself what the potential impact to the organisation is of not having these procedures and mitigation in place.

How to identify and measure the extent of your corruption and associated fraud risk

Proactive versus a reactive response to fraud and corruption allegations, which approach are you taking and what approach would you choose?

In trying to understand your corruption and associated financial crime risk, building a risk profile for your organisation including its insider threat is an important starting point in fighting fraud and corruption locally, throughout your organisation and its global supply chain.

> Create a culture of accountability where everyone takes responsibility for detecting and preventing procurement fraud.

Sources of data

If you are about to build a profile of your organisation risk, you should not only look at internal sources of information but also international assessment of risk that outline the current risks and themes that may impact your organisation.

One such source is the Report to the Nations published by the Association of Certified Fraud Examiners.

The 2022 ACFE study covered 2110 cases from 133 countries with a total loss of more than $3.6 billion. The average loss per case is documented as $1,783,000. A number of the key findings in this year's report include:

- corruption continues to be the most common scheme in every global region and is the most common scheme across all sectors
- 42% of fraud schemes were detected by tip
- organisations with hotlines detected fraud more quickly and lower losses that those organisations without a hotline
- nearly half of cases occurred due to the lack of internal controls or overriding existing controls
- only 6% of perpetrators had a prior fraud conviction
- 85% of fraudsters presented behavioural red flags of fraud

Are these areas that you're currently considering?

Concealment

Having an awareness of common fraud methodologies and associated risks are a necessary part in the detection and mitigation of risk. The report highlights that the top 5 concealment methods used by fraudsters included:

- 39% created fraudulent physical documents
- 32% altered physical documents
- 28% created fraudulent electronic documents or files
- 25% altered electronic documents or files
- 23% destroyed or withheld physical documents
- 12% of cases did not involve any attempt to conceal the fraud

The significant value in control measures can't be overstated, the ACFE research clearly highlights the importance of being able to collect your internal own internal data to detect and respond to fraud risk.

Although receiving tips is only one information source in building a risk profile, it is clearly a powerful tool. The findings also outline the common methodologies in which perpetrators commit fraud, that highlights the importance of training operational staff on what to look for in behaviours and most importantly where control measures are overridden.

When linked with staff that receives formal fraud training, the insider threat is clearly identified quicker and financial losses reduced, where an organisation is a target of fraud.

Proactive response to risk

So once you have a clearer picture of your risk, what is the next step? Do you introduce controls to mitigate these identified risks and then sit back and wait to see if they work or do you continually measure their performance? Are your policies and procedures, systems and controls or expertise and capabilities sufficient to identify and mitigate these risks?

To support this risk measurement are proactive detection techniques introduced, such as data analysis or audit to scrutinise the areas of risk that includes assessing whether common areas of risk within the procurement lifecycle or compliance programmes are a high, medium or low risk.

Do you recognise the value of data, the data sources that can be used to assess your risk and where to collect it. Are you confident on how data and its analyse can be used to drive your short, medium and long term approach to risk?

Preventing Corruption Insiders Guide Every Ethics Leader Needs

Are you able to measure the performance of your organisation's anti-corruption culture and is the coordination of your communication strategy and engagement with staff, partners and suppliers adequate enough to make an impact in reducing your bribery, corruption or procurement fraud risk?

> If we are to preserve culture we must continue to create it.
>
> — Johan Huizinga

To examine and understand an organisation's anti-corruption culture or whether it meets your belief or perception of its impact and how it protects organisation revenues, you must consistently measure performance against your organisation anti-corruption approach and communication.

Ethical response Vs anti-corruption culture

Where an organisation's ethical response doesn't match what it aspires to achieve in creating an anti-corruption environment then it is unlikely that it will be able to build a sustainable culture.

Where there is evidence of improper conduct or poor performance in dealing with ethical issues, then an unethical culture or behaviour is likely to be tolerated. This type of behaviour will limit the engagement and interest of staff or suppliers in reporting suspicions of fraud that will ultimately leave an organisation with a limited understanding of what its risk picture is. Examples of such behaviour might include:

- Ethical issues that are reported through line management that aren't addressed.
- Whistleblower reports that aren't appropriately dealt with or an individual is targeted by the organisation through bullying or intimidation.
- Improper treatment of suppliers or abuse of procurement route.
- Non compliance with procedures are common and aren't addressed.

Design out fraud

Where an organisation communicates a strong message that it takes corruption seriously, highlighting the types of corruption and associated fraud or financial crime that it is being targeted by, and where there is a proactive response, it communicates that there is a greater chance that individuals will be caught. In these circumstances, it is likely that fraud and financial loss will reduce. Key areas of communication an anti-fraud message might include:

- During the onboarding process, confirming conflicts of interest, ability to perform contracts and assessing a vendors own anti-fraud culture.
- Training and awareness provided to staff and suppliers that outline key typologies of fraud and where to report it.
- Ensuring that there are clauses within contracts that include anti-fraud and anti-bribery clauses, competition clauses to mitigate bid rigging, audit clauses, sub-contractor approval clauses
- Financial, procurement and quality controls including 5 way matches before invoices are approved.
- Ability of an organisation to receive and respond to reports of suspicions of fraud or irregularity from staff, suppliers or consultants.
- Strong recruitment procedures to ensure that individuals with conflicts of interest or fraud risk are identified.

Creating an anti-corruption culture

Enhancing the culture of an organisation requires the coordinated creation of a communication strategy that builds on various aspects of an organisations intention to engage all staff, partners and suppliers in its drive to identify and mitigate risk. When planning and developing a communication strategy to build organisational culture, a number of areas should be considered:

- Leadership, ownership and responsibility for the organisation's anti-corruption culture and strategy that includes demonstrating the tone from the top, setting an example for ethical conduct.
- Communication the reporting process with staff and suppliers, having a whistleblower protection policy and education and awareness that outlines an organisation's risk and their approach to mitigation.
- Internal engagement with staff that might include anti-corruption forums, having an anti-corruption platform and central library that hosts policies, messages and other communication.
- Supplier engagement including briefing, reporting process and visits to support their engagement with your organisation's as part of building supplier relationships.
- External engagement and communication including involvement with local, national or international forums to support and enhance an organisation anti-fraud focus.
- Anonymised feedback process that supports early risk identification and measurement of culture.
- Success measurement and performance indicators are an important part of monitoring and reporting positive outputs and development of the anti-corruption culture.

Conclusion

Communication and engagement with staff, suppliers, partners and third parties is integral in building an organisations anti-corruption culture. Publishing policies isn't enough and anti-corruption efforts should focus, not only on interaction with individuals but also look at how staff can be involved and drive an organisation's approach. After all, it is an organisations staff that understand where the challenges and weaknesses are within an organisations systems and controls.