



What Lies Beneath

The prevalence of and approaches to
procurement fraud in global business

2020 REPORT



Contents

FOREWORD	5
INTRODUCTION: PARTNERS IN CRIME	6
CHAPTER 1: HAS FRAUD BECOME NORMALIZED?	8
CHAPTER 2: DOES CRIME PAY?	10
CHAPTER 3: WHO SHOULD TAKE CHARGE?	12
AUDITING PRACTICES: BELIEF VS REALITY	14
THE OUTSOURCING PHENOMENON	15
CHAPTER 4: SUPPLIER INTEGRITY MATTERS	16
CHAPTER 5: WHERE IS THE PROCUREMENT FRAUD BLIND SPOT?	18
CHAPTER 6: ANALYTICS AND AI - THE POWER OF PROACTIVE PROTECTION	22
CONCLUSION: THE TIP OF THE ICEBERG	24



Foreword

By Ellen Roberson, CFE, Fraud, Anti-Money Laundering and Security Intelligence Adviser at SAS

Despite its prevalence and reputation, procurement fraud largely remains an unknown quantity. Whether your procurement process is compromised by a valued employee or a close supplier, organizations are often unwilling to pull back the curtain and discover what lies beneath.

E-procurement is seeing widespread adoption in markets across the world. However, implementation has not been equal everywhere and there are major discrepancies between markets when it comes to maturity. Furthermore, e-procurement isn't uncrackable in itself. Where there's a will there's a way, and fraudsters can avoid detection if organizations lack all the digitized contracts, invoices and analytics capabilities they need to keep track and interpret data quickly.

Procurement integrity isn't just important as a defense against fraud, it's a regulatory imperative. As the legislative landscape grows more complex, due diligence and the agility to respond to changing regulations is crucial to staying on the good side of regulators and customers. Indeed, 65% of procurement professionals consider regulation to be a growing threat to their business¹.

To beat procurement fraud, you have to modernize procurement itself. Don't wait for an incident to happen before looking for solutions. Annual or semiannual audits, which fraudsters can strategize around and undermine, cannot mimic the success of a continuous surveillance system. You must be proactive rather than reactive.

1. Dun & Bradstreet, *Compliance and Procurement Sentiment Report*, 2018, p.3.

INTRODUCTION

Partners in Crime

Procurement fraud is one of the most insidious and common forms of fraud today's organizations are likely to encounter. According to PwC, procurement fraud is one of the world's most commonly reported economic crimes, ranking above cybercrime and business misconduct². Yet, it is also one of the most elusive and taboo.

There is no single motivation that unites procurement fraudsters. A fraudulent supplier may be seeking a lucrative contract, while a disgruntled employee may only be interested in revenge. There is also no standard modus operandi, making procurement fraud harder to detect.

What isn't in question, however, is how damaging it can be. Procurement fraud puts the bottom line in jeopardy and can ruin an organization's reputation, embroiling it in legal battles for years to come. Tragically, it happens right under the noses of colleagues, with half of cases assisted by employees³.

It's estimated that organizations lose 5% of their annual revenues to fraud. What's more, the more senior the

perpetrator the more damaging the result. Indeed, the median loss caused by owners/executives was 17 times larger than the median loss caused by low-level employees⁴.

Beyond the initial fraud scope, many jurisdictions impose a mass of compliance requirements that can lead to serious fines if not adhered to. Regulations, such as the UK Bribery Act (2010), the French Sapin II (2017) and the US False Claims Act (1986), oblige companies to perform proper investigations into procurement and hold their employees to account.

However, the danger posed by procurement fraud shows no sign of abating. A general lack of awareness or concern in some countries, fears over reputational damage, and the absence of funds and visibility into procurement processes is creating a system that's easy to undermine. Slight regional differences and potential vulnerabilities in procurement practices – such as in Vietnam, South Africa and Uganda – only compound the issue.

2. PwC. *Pulling Fraud Out of the Shadows*. Global Economic Crime and Fraud Survey 2018.

3. Ibid.

4. ACFE. *Report to the Nations*. 2018 Global Study on Occupational Fraud and Abuse.



About Our Survey

Between 2018 and 2019, SAS and 3Gem surveyed 2,025 global business leaders across 38 countries for their opinions and experiences of procurement fraud. SAS commissioned the research to understand the extent of the problem and to assess how well organizations understand it and attempt to fight back. The goal was to analyze current anti-fraud strategies, while making the case for a more analytical, technology-enabled approach.

CHAPTER 1

Has Fraud Become Normalized?

Procurement fraud covers a broad range of illegal practices. We asked respondents to consider a number of different types of internal and supplier malpractice – from contract bid rigging to travel and expenses fraud and invoice splitting – to gauge its prominence and what form it usually takes.

Occupational fraud, meaning the use of one's occupation for personal enrichment through the misuse of resources, emerged as the most widespread in global business. In particular, travel and expenses (44%) and small acquisitions fraud (29%) ranked highly in this area. Employee-focused fraud is especially prevalent in East-Asian markets: 80% of Malaysian organizations and 60% of Singaporean companies have dealt with travel and expenses fraud.

This is perhaps unsurprising as in many cases it is easier to detect than fraudulent behavior committed by external vendors. Employee fraud (particularly expenses) may also be better understood and more "front of mind" than procurement. This focus, however, may be detracting attention from the very real threat of procurement fraud.

Contract bid rigging was the second most common fraud type globally with over a third (34%) of businesses having experienced it. It is also the most prevalent in some surprising markets: 64% of organizations in New Zealand and Hong Kong have experienced it, closely followed by Canada (58%). However, there is a strong chance these markets simply have better detection processes.

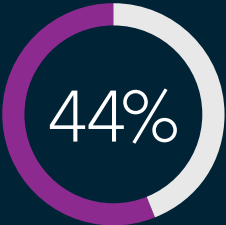
By contrast, the occurrence of contract bid rigging appears very low in South American countries: Argentina (8%), Columbia (16%), Brazil (22%). These are major developing countries, so the occurrence of fraud is likely much higher than reported.

Invoicing practices were also popular targets for fraudsters. Duplicate invoicing appears to be an all-too-common practice, experienced by 28% of businesses, while 22% have seen suppliers splitting invoices fraudulently to avoid controls. Collusion is crucial to the success of these kinds of fraud. Almost a quarter of organizations have experienced collusion between suppliers (23%) and collusion between employees and suppliers (24%).

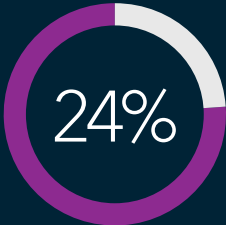
The commonality of procurement fraud across the globe could be considered surprising: getting caught can result in a jail sentence in many countries. Yet, regardless of the potential punishments, there are people and companies willing to take the risk.

Perhaps the most compelling statistic when we look at the types of procurement fraud that had been witnessed was not the numbers attached to each one, but instead the even spread across a number of different categories. At first glance organizations may assume that the cost of occupational fraud will be less than threats such as ghost suppliers, but they can't afford to overlook anything.

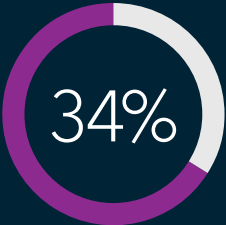
THE MOST COMMON VARIETIES OF INTERNAL FRAUD, RANKED IN ORDER



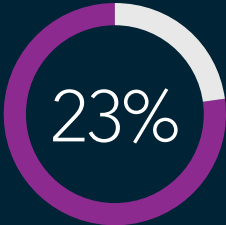
TRAVEL AND EXPENSES



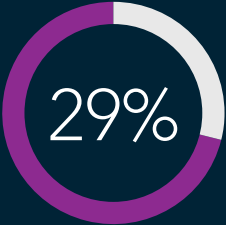
COLLUSION BETWEEN EMPLOYEE AND SUPPLIER



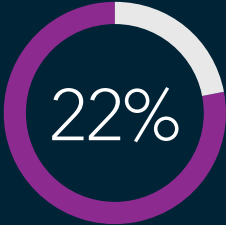
CONTRACT BID RIGGING



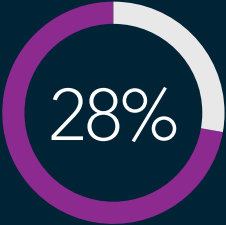
COLLUSION BETWEEN SUPPLIERS



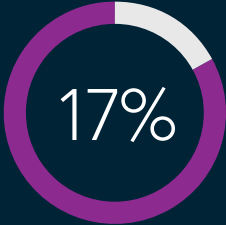
SMALL ACQUISITION PURCHASING



INVOICE SPLITTING



DUPLICATE INVOICING



GHOST SUPPLIER

CHAPTER 2

Does Crime Pay?

The true scale of the financial damage caused by procurement fraud will inevitably be masked by a degree of underreporting. You can't assess what you don't detect, and irregularities may be overlooked, conflated or suppressed internally. Some victims, and colleagues of the perpetrators, may decline to reveal the true scale of fraud losses to protect their company's reputation.

Still, it is shocking that a third of businesses (33%) don't seem to know how much they lose to procurement fraud each year. This includes a fifth of respondents that assume their losses are negligible, but which can't give an estimated amount. This suggests a culture of negligence or ignorance in many organizations. If a third are unable to provide exact losses, the actual problem is no doubt much greater than reported.

However, the picture varies from region to region. Canada is the most rigorous country when it comes to understanding and reporting losses from procurement fraud - only 2% admit to not knowing how much it costs them each year.

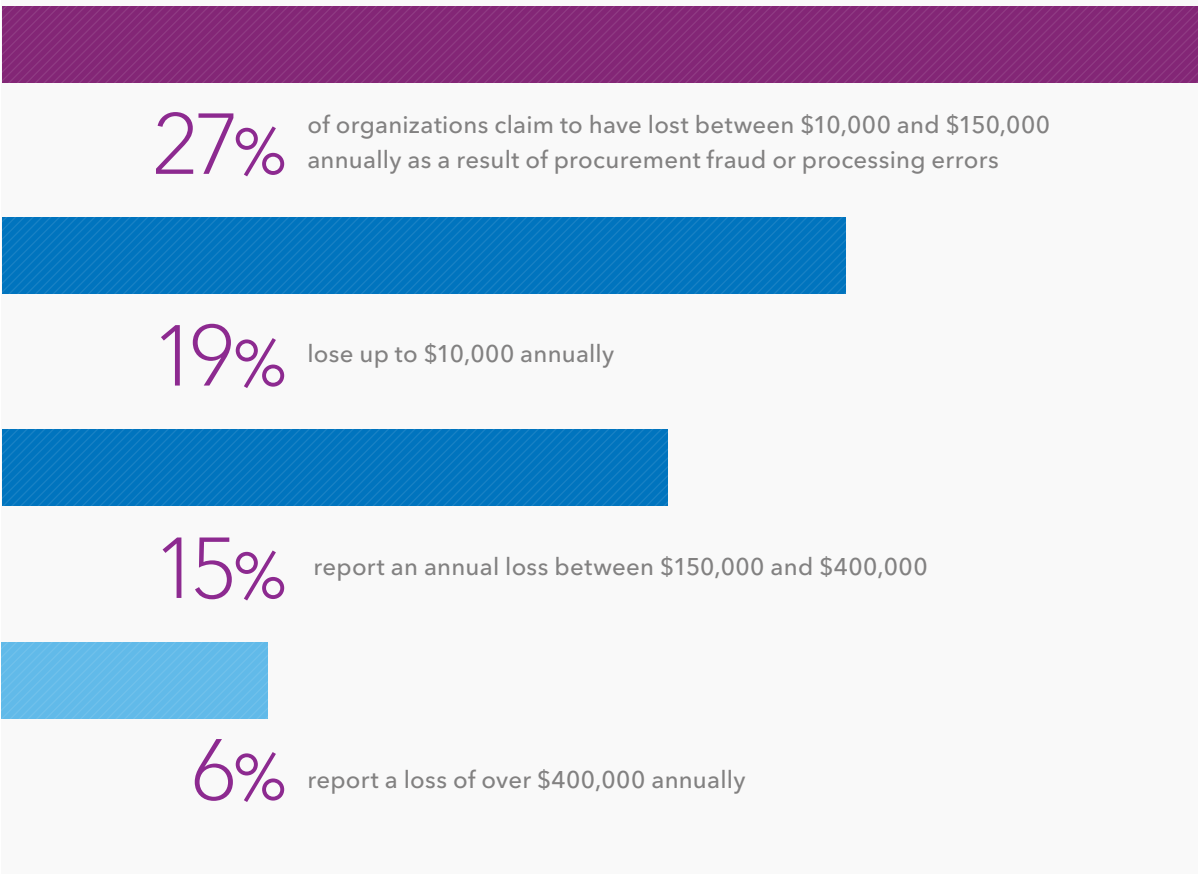
Meanwhile, Asian markets appear to have the poorest record of keeping fraud costs under control. In Taiwan and the Philippines, 28% of organizations assume their losses are negligible. In Japan, 26% of companies

assume their losses are small and, shockingly, 30% have no understanding of how much it costs them. That's more than half (56%) of Japanese companies that can't say how much they are losing to procurement fraud.

When we look at those organizations that didn't select "negligible" or "don't know" we can see that the most frequently reported amount lost was between \$10,000 and \$150,000 annually (27%). This is a significant amount, and seems to align with estimates of average losses of 5%. These numbers are of course relative to the size of the organization, but it's clear that procurement of goods and services accounts for a large share of organizational expenditures.

However, there is no clearly defined floor or ceiling to fraud losses. In this respect, Taiwan appears to be the most expensive market for procurement fraud in the world. A quarter (24%) of Taiwanese organizations claim to lose over \$400,000 annually. By contrast, Indonesia and Peru report the lowest losses to procurement fraud, with 44% in both countries claiming to lose no more than \$10,000 annually. However, minimal losses just as likely reflect underreporting as they do the reality of fraud.

HOW MUCH MONEY IS LOST DUE TO PROCUREMENT FRAUD OR PROCESSING ERRORS?



27% of organizations claim to have lost between \$10,000 and \$150,000 annually as a result of procurement fraud or processing errors

19% lose up to \$10,000 annually

15% report an annual loss between \$150,000 and \$400,000

6% report a loss of over \$400,000 annually

Ultimately, any and every industry is in the firing line for procurement fraud. Good business depends on a good reputation, but revelations about fraud can tarnish this. "Ethical" companies delivered a 7% higher return on equity during the last five years than other companies on the Russell 1000 index⁵.

Reputations can recover over time. However, as business leaders focus on fraud cases, other priorities may slip, resulting in further business damage. Procurement fraud continues to do harm long after it's discovered.

5. Just Capital, *Looking for strong returns? Ask the American people*, 2018, p.5.

CHAPTER 3

Who Should Take Charge?

With procurement fraud so widespread and destructive, clear leadership is needed to successfully tackle it. Without someone to take responsibility, standards drop and individual cases can easily avoid attention.

However, our data shows that there's urgent room for improvement in this area. Across the world, there is no shared approach to procurement fraud prevention, with many organizations reporting multiple owners. Often it is a matter of finger-pointing, with few willing or confident enough to take responsibility for procurement fraud, resulting in a weaker defense overall.

Without consensus, responsibility differs considerably between companies. One-third of organizations (33%) choose the most popular option - assigning responsibility to the finance function. This is understandable considering they have responsibility over the financial health of the organization. If fraud succeeds, the buck stops with them. However, this doesn't mean the CFO takes the lead in day-to-day anti-fraud efforts, or is well-equipped to.

The head of procurement was the next most popular option (23%), followed by internal auditors (19%), business or departmental heads (17%) or legal (13%). Over one in 10 (11%) claim responsibility is shared across departments, but that adds up to a fifth (19%) of

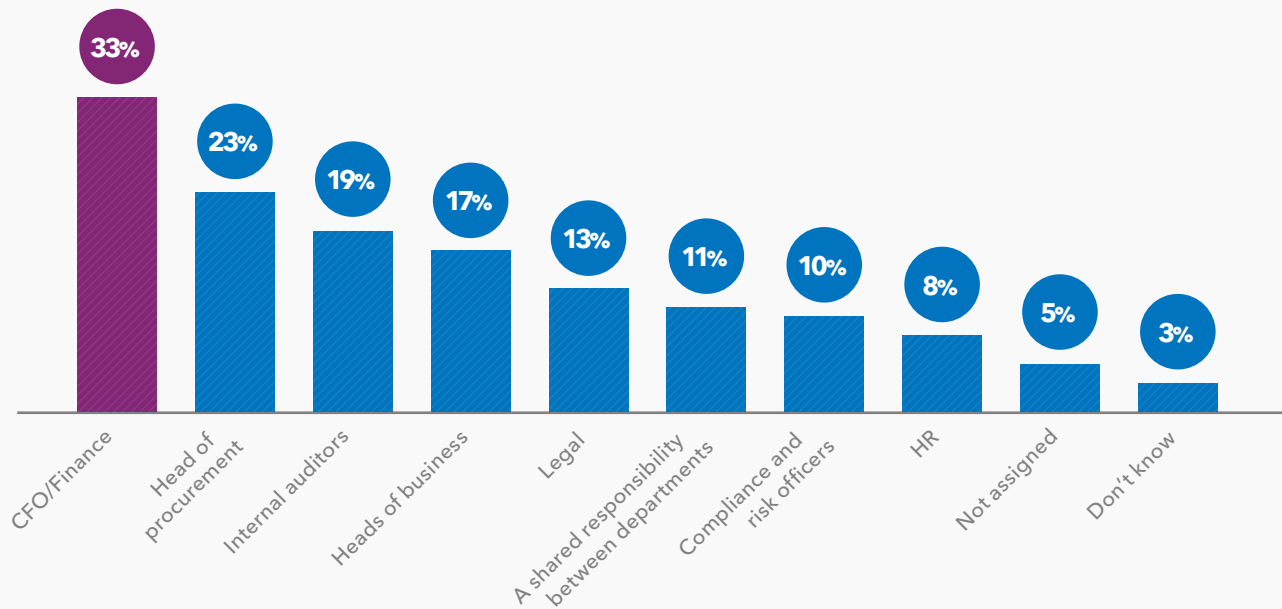
organizations in total with no clear personnel assigned to the task. This lack of agreement suggests that many businesses do not take procurement fraud seriously.

Responsibility for fraud in the workplace is a careful balancing act. Overall responsibility and strategic decision making are crucial, but all activity shouldn't be confined to one department. Finance departments, for example, may approach procurement first from a commercial rather than an ethics or accountability viewpoint.

Responsibility for uncovering fraud should be embedded throughout the workplace. Every employee in every department should be vigilant and encouraged to come forward with their suspicions. For medium-to-large organizations, a dedicated fraud team - tasked solely with the detection and resolution of potential fraud - is strongly advised.



WHO IS RESPONSIBLE FOR DEALING WITH POSSIBLE FRAUD IN PROCUREMENT?



Auditing Practices: Belief vs. Reality

Audits into company accounts are crucial for uncovering error and potential wrongdoing during procurement. How often a company undertakes these investigations is a useful indicator for its awareness of the threat and its willingness to see it resolved.

Businesses seem to recognize the importance of audits on a surface level. Our data shows they overwhelmingly rely on regular internal audits (58%) to identify cases of fraud. However, what organizations defined as "regular" varied drastically between regions and is in need of some reassessment.

Annual audits proved to be the preferred option, used by 25% of respondents. Under a fifth (17%) told us they carried out quarterly audits while 16% did them twice a year. Only 6% performed them on an active ad hoc basis as required.

This suggests that many organizations are operating under a false sense of security, believing their auditing strategy is robust but not being done regularly enough to catch ongoing threats. To illustrate, over half (65%) of Canadian companies claim to hold regular audits into procurement fraud, but only 2% do it ad hoc as needed.

More disturbing, however, is that over a quarter (26%) of global businesses claimed they didn't audit for procurement fraud at all or admitted that they didn't know if or how often they audited for it.

This lack of frequency will have a significant impact on organizations. The bigger the gap between audits, the longer procurement fraud will take to be spotted.

By this time, the damage will already have been done. It also makes it less likely that ongoing fraud will be detected in progress, making any losses greater in scale.

The methods for detection are equally concerning. When we look at how organizations deal with procurement fraud, more than a third (36%) validate procurement applications manually, with 28% of them relying on staff to inform them of any wrongdoing. There is a significant risk of human error and potential tampering in both approaches.

However, there are also definite positives to note. More than a third (37%) use some form of data analytics to detect instances of procurement fraud. This approach is far more likely to uncover subtle irregularities in the data set that manual methods likely miss. It can also be run consistently without the need for constant human labor. Yet, while many organizations are heading in the right direction, there is an undeniable reliance on manual methods and regular auditing processes are lacking.

When audits are infrequent and the rules and schedules well-known, they are little more than a bandage. Fraudsters can easily exploit their knowledge of the auditing timetable, ensuring compliance during and in the buildup to the audit. But they start again as soon as the auditors have gone. This process can continue for years without the fraudster ever being caught. The solution to this quandary lies in a more advanced approach: continuous monitoring based on advanced analytics.



The Outsourcing Phenomenon

As many as 15% of organizations outsource the procurement process to external auditors, while 10% rely on a third-party organization for their annual audit. There are some clear advantages to this strategy, especially in regards to occupational fraud. External auditors are more likely to be objective and not downplay issues in procurement practices. They will also be more detached from the office politics of their customer, and are more likely to view all employees with an equal level of scrutiny.

However, dangers still remain. Businesses should look carefully at the credentials and history of a potential auditor before signing them on. An external auditor does not guarantee an air-tight detection process. The 2009 collapse of Alabama's Colonial BancGroup has been attributed partly to the failure of PricewaterhouseCoopers in uncovering fraud taking place at the Federal Deposit Insurance Corp⁶. Even when outsourcing procurement fraud detection, supplier due diligence is essential.

This doesn't change the fact, however, that remote processing is a good place to start for organizations without the capabilities to run their own regime with confidence. The practice can serve as an eye-opener, showing organizations what's possible when data analytics is applied to fraud detection. However, in time, it is best for the organization itself to take responsibility and bring the procurement process in-house.

6. Bloomberg, PwC to Pay \$335 Million in Settlement Over Audits of Failed Bank, 2019.

CHAPTER 4

Supplier Integrity Matters

Internationally, growing pressure is being placed on companies to ensure they are working with legitimate suppliers not affiliated with any sanction lists. Increasingly, supplier due diligence is also becoming a key concern for compliance departments and personnel. The latest US Department of Justice compliance guidelines⁷ highlight procurement and supplier integrity as a key area for prosecutors determining whether an organization's practices are legal and compliant.

Going into procurement with the right mindset and priorities can help companies make the best choice of supplier, both commercially and ethically. Avoiding procurement fraud is about requiring the same high ethical standards from suppliers as you do from employees, as well as careful vendor analysis.

When choosing a new supplier, companies consider quality of product or service, cost and industry recognition to be the most important factors in their decision. However, it's positive that as many as 1-in-10 businesses consider the supplier's record of fraud or errors (10% and 7% respectively) as the decisive factor. Although this is not represented in the rest of the data set.

A comprehensive supplier due diligence process should sit at the heart of every project or transaction, but organizations aren't performing it regularly enough. The majority monitor their supplier network quarterly (24%), twice a year (21%) or annually (21%). Less than a tenth (9%) perform due diligence every time they begin a new project or transaction.

It's understandable that fraud isn't the first thing on purchasers' minds when they select suppliers. However, neglecting supplier due diligence could prove a costly mistake if the decision makers make a bad call. By contrast, an analytics solution that proactively analyzes the market and any new suppliers has the power to highlight potential fraud before it begins. A year or even three months is too long before you detect an ongoing fraud activity.

7. US DoJ Criminal Division, Evaluation of Corporate Compliance Programs, 2019.



CHAPTER 5

Where Is the Procurement Fraud Blind Spot?

Beyond auditing and procurement practices, it's the technologies used for detection which make the biggest impact on fraud defense. Yet, fraud detection is too often considered a low or unnecessary priority in procurement. Nearly a tenth (7%) don't monitor their procurement processes at all. However, it's both naive and dangerous to assume it isn't needed.

Globally, many organizations do invest in procurement fraud detection, but are let down by their tools and techniques. For those that do actively monitor for procurement fraud, the majority are over-reliant on manual processes (50%) or rule-based detection software (38%). Neither method can provide reliable or consistent protection.

Manual controls can introduce human bias and error into your system. Any employee or business leader can turn out to be a fraud actor, but many can avoid suspicion due to popularity or seniority in the business. Indeed, the typical fraudster profile in an organization is male and in a position of authority. In 2017, 70% of corruption cases involved someone in a managerial or owner/executive position, and 82% of all corruption instances were committed by men⁸.

Considering the lack of clear accountability for fraud prevention, it is unlikely those performing manual controls consider it to be their primary role. Inevitably, corners will be cut, and other tasks prioritized, making it all too easy for fraudulent behavior to slip by undetected.

Detection software tends to be more objective than manual controls, but the implementation is often rudimentary and rules-based. The technology casts a wide net, catching innocent accidents or anomalies alongside genuine signs of fraud. False positives like these consume time and resources while the actual fraud continues in the background. Furthermore, anyone with knowledge on how the rules behind the software operate may easily find strategies to avoid detection.

It's positive, however, that a sizeable contingent (24%) are using a form of advanced analytics in their detection. Analytics can drastically boost the speed and success rate of detection, quickly and efficiently resolving vast data sets that would cause human investigators to struggle. This hopefully indicates a trend of organizations coming to recognize the

8. ACFE. *Report to the Nations*. 2018 Global Study on Occupational Fraud and Abuse.

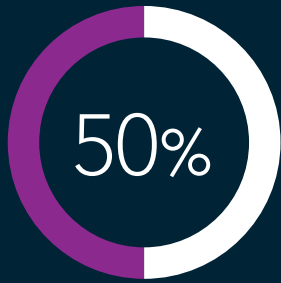
capability of analytics to uncover and prevent procurement fraud. However, those who appreciate its utility still represent a small part of the global community.

Ultimately, it's AI and automation technology that hold the key to leveling up organizations' procurement fraud defenses. Yet this is the least popular method for organizations, used by less than a fifth (17%). This could be due to a lack of understanding of the technology and its potential application in fraud prevention.

Procurement fraud can take place at any point during the procurement cycle, making it extremely difficult to investigate and detect. Manual audits and rule-based software can only go so far, relying on auditor skill and blunt rulings to detect fraudulent behavior from within a large set of data. Current defenses cannot provide the continuous monitoring needed to stay on top of procurement fraud at all times.

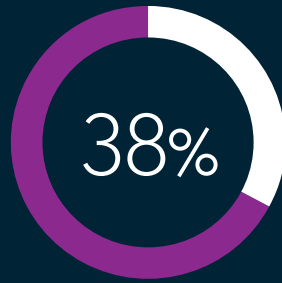


HOW DO YOU MONITOR PROCUREMENT PROCESSES FOR FRAUD?



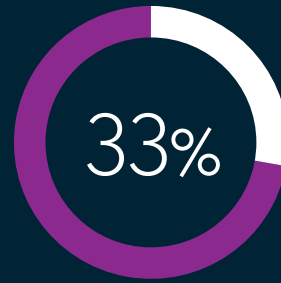
MANUAL CONTROLS

A member of staff manually checks Excel spreadsheets and paper documents for possible errors and suspicious behavior.



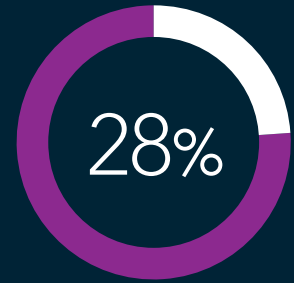
BUSINESS RULES

Software-based technology detects when, for example, somebody tries to send a payment below a threshold or splits an invoice to avoid controls.



ANOMALY DETECTION

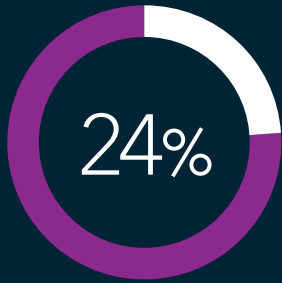
Software-based tools detect if a supplier is paying invoices late or at an unusual date outside of the contracted period.



DATA INTEGRATION & CLEANSING TECHNOLOGY

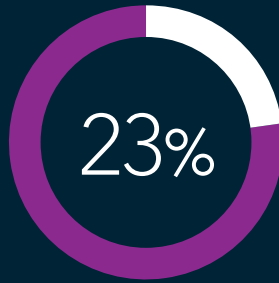
Data management applied across multiple platforms and operating systems can correlate and deduplicate data.

HOW DO YOU MONITOR PROCUREMENT PROCESSES FOR FRAUD?



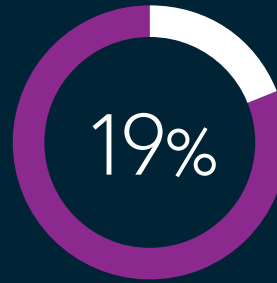
ADVANCED ANALYTICS

Algorithm-based technology, including machine learning, is used to analyze statistical and text-based information to identify trends and score the level of risk of a supplier, third party, invoice, purchase order and collusions between entities.



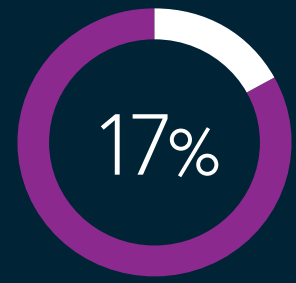
USER ACCESS CONTROLS & SEGREGATION OF DUTIES

Preventive analytics software protects sensitive information and data by managing user accounts and access privileges.



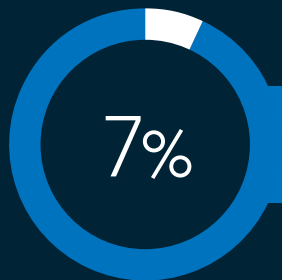
TEXT ANALYTICS

Software-based tools analyze text data from documents and databases to determine the similarity between two invoices (for example).



ARTIFICIAL INTELLIGENCE (AI) & AUTOMATION

The combination of predictive analytics with computer vision and natural language processes are used to forecast and optimize detection monitoring, with self-learning capabilities.



DON'T MONITOR PROCUREMENT PROCESSES

CHAPTER 6

Analytics and AI – The Power of Proactive Protection

Continuous, data-driven detection is the best way to fight procurement fraud. It enables companies to preempt fraud rather than simply discover it after the fact. This reduces costs, saves time and prevents losses.

Sadly, few companies today are using the best tools available for the job. A minority utilize advanced analytics (24%) and AI (17%) in their anti-fraud efforts. Canada and New Zealand lead the pack when it comes to these leading-edge technologies: Respectively, 48% and 40% use advanced analytics, while 40% and 20% use AI. China is also a strong performer, with 36% of companies utilizing advanced analytics and 38% using AI.

Organizations provide a number of justifications for not taking advantage of such techniques. Perceived cost leads the way while a lack of skills is also considered a challenge. A concerning 29% prefer to use manual detection techniques despite their considerable drawbacks. An alarming 14% of respondents did not believe advanced anti-fraud tools were necessary, because they had never been victims.

It's clear that the challenges holding companies back are not solely material or technological, but psychological as well. Businesses should reconsider objections based on cost, prioritizing options based

on potential ROI. Implementing advanced analytics and AI will of course require an upfront cost, but these solutions quickly pay for themselves in the fraud threats they neutralize.

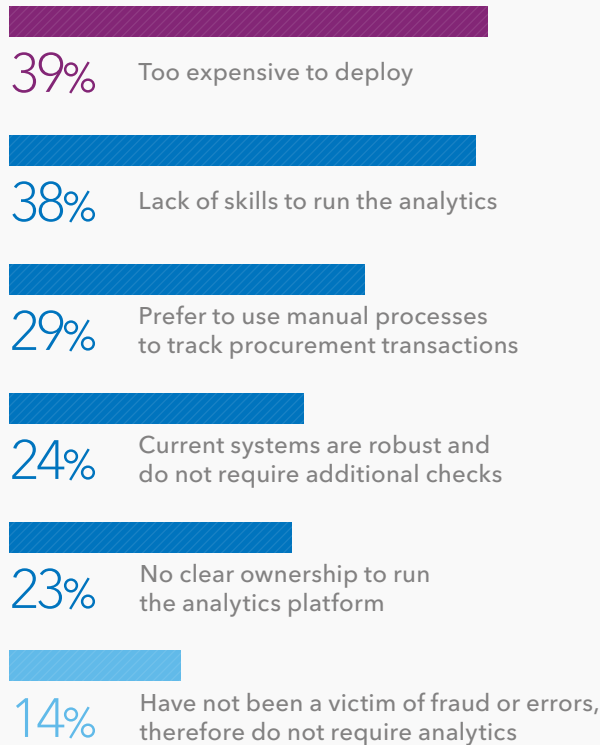
One of the major challenges fraud teams struggle with is the amount of data that needs to be analyzed for fraud detection. Yet, machine learning and AI have the capabilities to do this quickly and consistently while also saving money for the organization.

These technologies can pick up on data points and the subtle signs of fraudulent activity that too often go unrecognized by investigators. By performing much of the analytics workload and reducing the number of false positives, a more sophisticated detection system also gives employees time to focus on more complex, high-priority tasks.

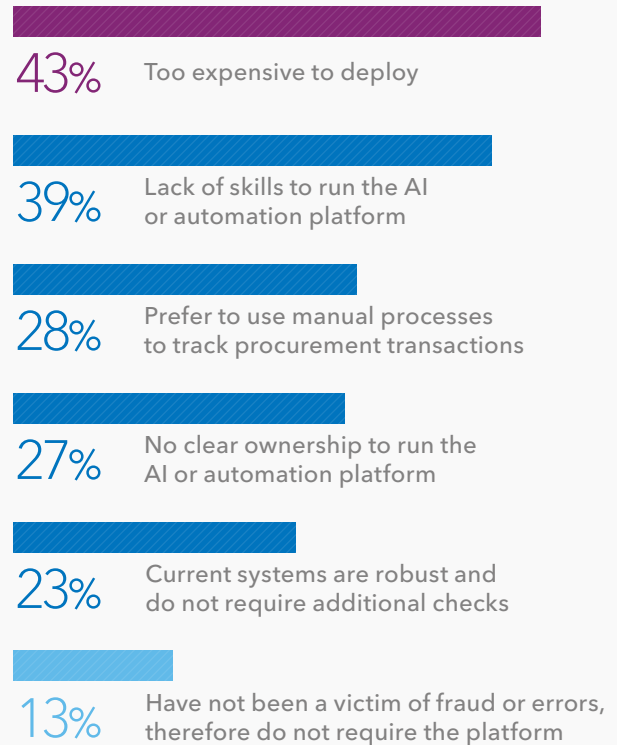
AI and analytics are also crucial from a damage limitation perspective. By detecting threats in progress, they can help stop procurement fraud upstream before its perpetrators can do significant damage. This is the key advantage the technologies hold over other forms of fraud protection – they enable companies to preempt fraud rather than simply discover it. Additionally, being able to demonstrate a proactive approach to fraud detection may make the organization more

What's holding fraud protection back?

THE TOP BARRIERS TO ADVANCED ANALYTICS



BARRIERS TO AI



attractive to prospective buyers and customers. This is another way that fraud prevention pays for itself.

In particular, the 14% of companies who do not believe they have been victims of fraud or errors should

seriously reconsider their processes. With 33% of companies unable to report how much fraud is costing them and 26% not investigating procurement fraud at all, they could easily be unwitting victims.

CONCLUSION

The Tip of the Iceberg

The world is failing to put up a united defense against procurement fraud, which remains pervasive yet also elusive. But in many markets, the threat of procurement fraud is viewed very seriously and steps are being taken to tackle it. Countries, including Canada and New Zealand, report high instances of fraud and they have equipped themselves with the tools to put a stop to it.

By contrast, the threat posed by procurement fraud is not widely acknowledged in South American countries, which report low occurrences across the board. In some East-Asian markets, especially in Japan, procurement fraud could well be systemic. Little is known of its true extent and the steps taken to tackle it are limited: 31% of Japanese companies admit to not monitoring for procurement fraud at all.

Until organizations adopt an integrated, data-driven approach, millions will continue to be lost to procurement fraud. Analytics capabilities are crucial to identifying and catching people trying to dodge existing controls and procedures. By using the latest advanced analytics and AI solutions, anti-fraud teams can sift through huge quantities of data effortlessly. Anomalies and patterns can be detected quickly, enabling businesses to immediately take action.

Of course, most organizations will need to learn how to walk before they can run. Taking on a full, on-site implementation of an advanced anti-fraud solution could be hard to justify for less analytically mature companies. A temporary approach relying on services from a vendor is one option. Or, organizations can attempt to build up their analytics capabilities over time.

You don't need to have costly, in-house specialists to take advantage of AI and machine learning techniques. Look for analytics solutions that provide explanations in business terms and are accessible to all skill levels. Automating the detection process is a sure way to reduce errors and false positives. By combining data analytics with AI, you can do more than detect and fight procurement fraud - you can catch it before it starts.



For more insight into procurement integrity, visit
www.sas.com/procurement-integrity

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are trademarks of their respective companies. © 2020, SAS Institute Inc. All rights reserved. 111248_123663.0320

