"Examining the risk of fraud, corruption, collusion, and manipulation"

PROCUREMENT AND TENDER FRAUD

February 2024

23rd Edition

RMG™

Content

Economic downturns “create” opportunities for fraud	3
Key procurement fraud schemes	4
Procurement fraud red flags	6
Weakened anti-fraud controls	7
Vendor pressure	7
Fraud risk mitigation strategy	8
Proactive due diligence is vital	9
Capability offered by solutions such as a Commercial Crime Vendor Management Systems	10
Transition from reactive fraud prevention to proactive fraud risk management	11
A holistic commercial crime prevention approach at all levels of business	12

Procurement and the tender process are prime targets for fraud, corruption, collusion, and manipulation. With large sums of money involved, opportunities are abound for unscrupulous employees, suppliers, and contractors to engage in illicit activities for financial gain. Organisations can face major financial, legal, and reputational damages if procurement fraud hazards are not adequately identified and controlled.

Economic downturns "create" opportunities for fraud

Periods of economic decline increase the risk of procurement fraud. Tighter budgets, reduced revenues, and uncertainty magnify the incentives and pressures to engage in fraudulent activities. Cost-cutting initiatives, staff reductions, and lowered oversight due to constrained resources weaken anti-fraud controls when risks are heightening.

Suppliers face greater financial pressures as business contracts and opportunities for collusion expand as vendors fiercely compete for shrinking budgets. The convergence of pressures, motives and opportunities during downturns create a perfect storm for procurement fraud.

Without vigilant prevention and detection measures in place, organisations leave themselves highly vulnerable to potentially significant damages from procurement fraud during turbulent economic conditions. Losses from corruption, kickbacks, bid rigging, inflated pricing, and payment schemes can quickly escalate.

"A leopard does not change its spots"

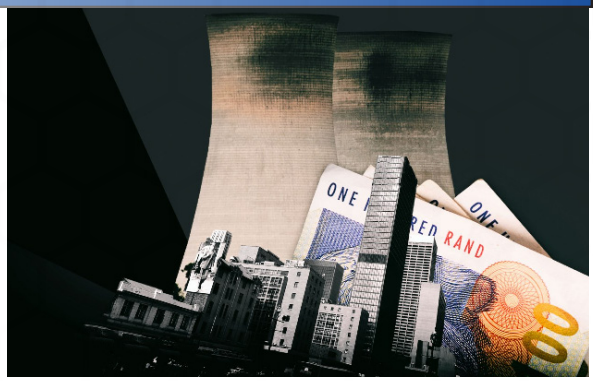
Key procurement fraud schemes

Bid Rigging

Bid rigging involves collusion amongst bidders to manipulate the bidding process. This can take forms such as bid suppression, complementary bidding, bid rotation, and subcontracting arrangements. The aim of this unethical behaviour is to control the outcome and eliminate true competition from the process.

Inflated Pricing

Vendor and employee collusion to artificially inflate pricing is a common fraud phenomenon. This may entail marking up invoices, charging for undelivered goods or services, or vendors providing kickbacks to the employees involved.



Billing Schemes

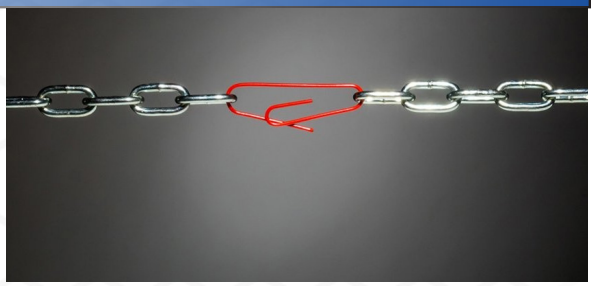
False invoicing, duplicate invoicing, and charging for goods not received or services not rendered are billing schemes aimed at extracting payments from the organisation illegitimately.

Inventory and Payment Diversion

Company assets like inventory, equipment, and payments can be illicitly diverted to vendors, staff, or third parties for personal gain.

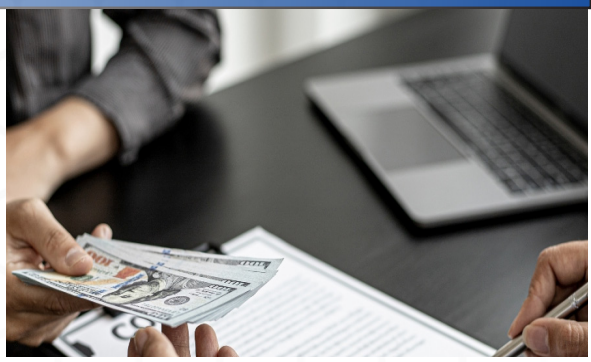
Substandard Materials

Suppliers may collude with staff to supply inferior materials or products and pocket the cost differences. Without proper controls, these schemes are difficult to detect.



Unauthorised Purchases

Employees may make unauthorised or fraudulent purchases outside of normal procedures, often in cahoots with vendors. These purchases are difficult to identify without strong oversight.

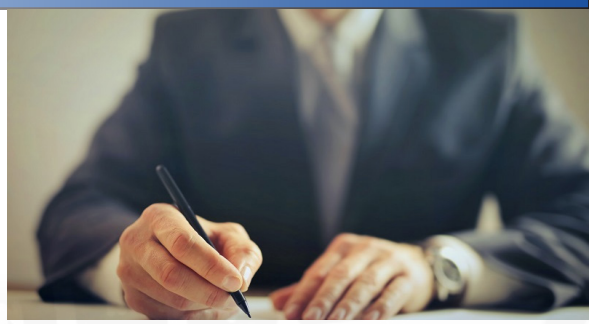


Corruption and Kickbacks

Suppliers or contractors may bribe staff with cash, gifts, trips, entertainment, or other incentives to obtain business or inflate costs. Recipients may facilitate overpayments or process fraudulent transactions.

Manipulation of Specifications

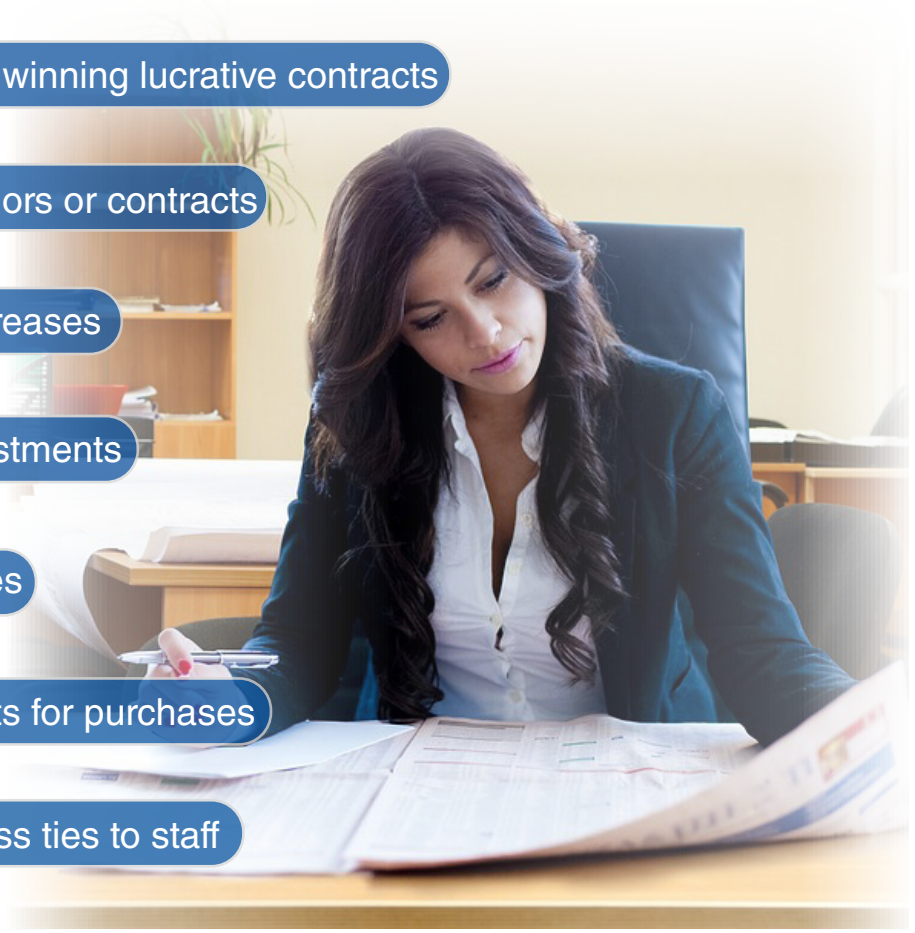
Tailoring requirements and specifications to favour certain bidders is an illicit tactic staff may employ if compromised. This shuts out true competition.



Procurement fraud red flags

Certain indicators can act as red flags for potential fraud risk identifiers in procurement:

- Sudden change in buying patterns, vendors used, or drastic volume variances
- Vendors with little experience winning lucrative contracts
- Staff resisting rotation of vendors or contracts
- Unexplained vendor price increases
- Inventory shortages and adjustments
- Duplicate payments or invoices
- Missing supporting documents for purchases
- Vendors with family or business ties to staff
- Poor segregation of duties
- Lack of oversight and monitoring



- Heightened motives during economic decline - To mitigate the risks associated with heightened motives during economic decline, organisations should implement robust measures such as increased oversight, regular audits,and reinforcement of ethical standards.

Turbulent economic conditions substantially amplify financial motives for vendors, employees, and contractors to engage in illegal profiteering schemes:

Vendor pressure

- Increase in expenses and decline in revenue
- Declining sales volumes and revenues
- Tighter margins and cash flow constraints
- Intense competition for limited contracts
- Existential threats for struggling businesses
- Employee pressure
- Job insecurity and reduced bonuses/raises
- Need to supplement income amidst belt tightening
- Greed providing rationalisation to commit fraud

With their livelihoods under threat, unethical vendors and employees find it easier to justify “cutting corners” for financial gain, and the risks of getting caught may seem smaller relative to the potential rewards and justified and rationalised with the inability to address fraud and corruption by the government.

Weakened anti-fraud controls

In addition to heightened motives, organisations often compromise their procurement fraud controls during times of economic distress:

- Cost cutting reduces fraud prevention budgets
- Staff downsizing leaves less oversight on vendors
- Pressure to reduce spending may lead to shortcuts
- Poor segregation of duties increases vulnerabilities

The very risk management and compliance functions meant to deter fraud are often weakened when risks increase. This perfect storm requires heightened vigilance to avoid spiralling fraud, losses and reputational damages.

Fraud risk mitigation strategy

Despite budgetary pressures, organisations must prioritise investment in procurement fraud prevention and implement robust risk mitigation strategy:

- Procure supplier fraud risk assessment services
- Perform thorough vendor due diligence procedures
- Incorporate four-way match controls (purchase order, receipt, invoice, payment)
- Maintain master vendor lists and transaction records
- Require compulsory competitive bidding
- Institute automated invoice and payment controls
- Maintain purchase order system with approvals
- Enforce stringent conflict of interest policies
- Update conflict of interest declaration quarterly
- Provide staff fraud awareness training
- Provide staff ethics training
- Conduct regular audits on procurement activities
- Implement analytics to detect patterns and outliers
- Establish independent whistleblower reporting channels
- Vigilance must increase during downturns

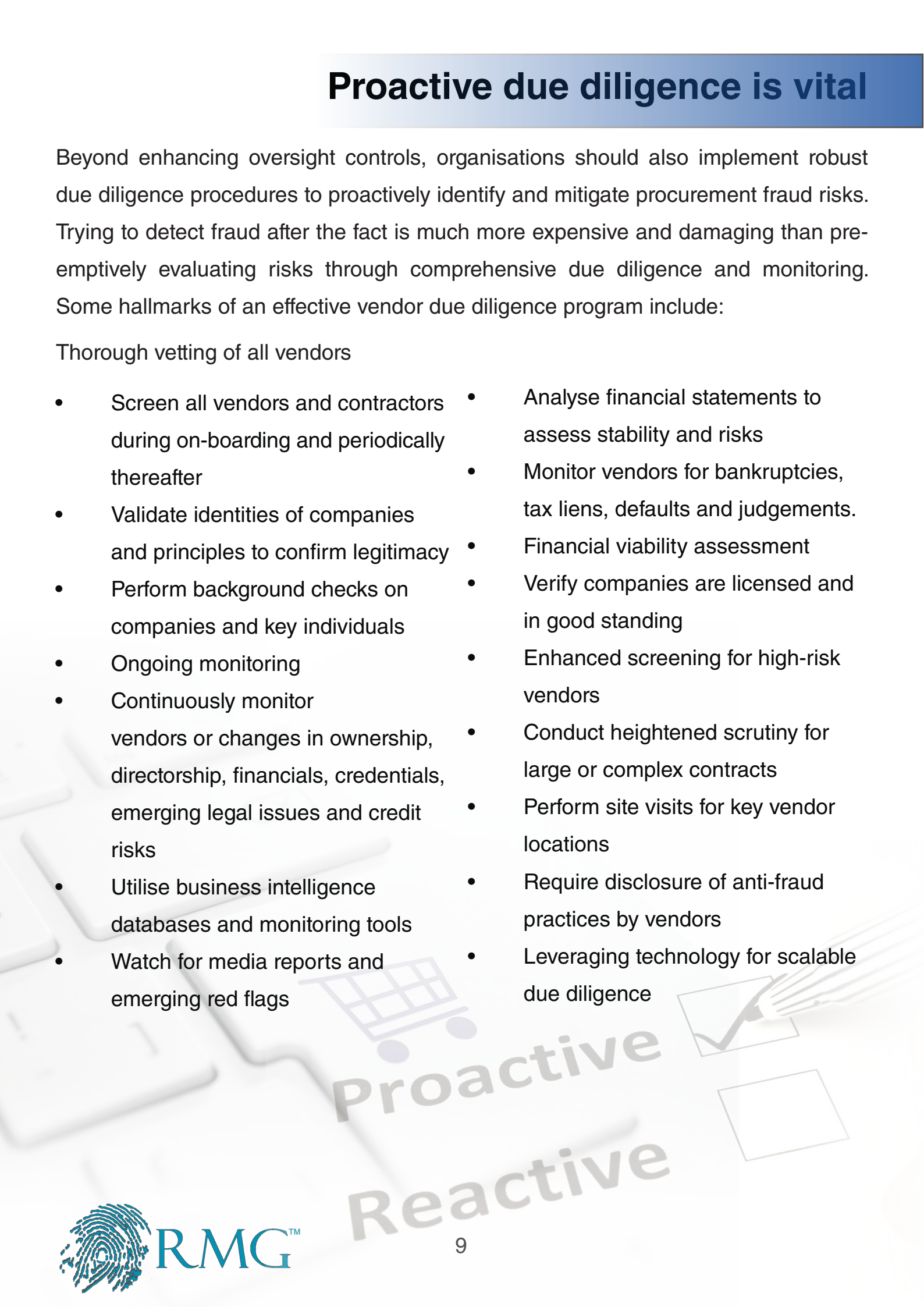
In economically challenging times, procurement fraud vulnerabilities paradoxically increase while organisations are tempted to scale back oversight and anti-fraud investments. However, vigilance and prevention must intensify during periods of heightened risk. The short-term savings from fraud prevention budget cuts are trivial compared to massive financial and reputational damages from procurement fraud reaching epidemic scale.

Proactive due diligence is vital

Beyond enhancing oversight controls, organisations should also implement robust due diligence procedures to proactively identify and mitigate procurement fraud risks. Trying to detect fraud after the fact is much more expensive and damaging than pre-emptively evaluating risks through comprehensive due diligence and monitoring. Some hallmarks of an effective vendor due diligence program include:

Thorough vetting of all vendors

- Screen all vendors and contractors during on-boarding and periodically thereafter
- Validate identities of companies and principles to confirm legitimacy
- Perform background checks on companies and key individuals
- Ongoing monitoring
- Continuously monitor vendors or changes in ownership, directorship, financials, credentials, emerging legal issues and credit risks
- Utilise business intelligence databases and monitoring tools
- Watch for media reports and emerging red flags
- Analyse financial statements to assess stability and risks
- Monitor vendors for bankruptcies, tax liens, defaults and judgements.
- Financial viability assessment
- Verify companies are licensed and in good standing
- Enhanced screening for high-risk vendors
- Conduct heightened scrutiny for large or complex contracts
- Perform site visits for key vendor locations
- Require disclosure of anti-fraud practices by vendors
- Leveraging technology for scalable due diligence



Traditional manual due diligence procedures often fall short, as they are resource intensive, inconsistent, and lack comprehensive data validation. Modern cloud-based vendor risk management technologies on the other hand, enable automation, streamlining, and enhanced intelligence powered by Big Data) analytics.

Capability offered by solutions such as a Commercial Crime Vendor Management Systems include:

Unified vendor risk database

- Centralise supplier data into a single searchable system
- POPIA Compliance
- Consensual maintenance of documentation such as financials, licences, policies
- Identify high-risk entities through relationship mapping
- Automated due diligence workflows
- Configure rules-based processes to standardize procedures
- Digitally collect and verify vendor documentation
- Auto-generate compliance status alerts and reports
- Ongoing monitoring alerts
- Flag changes in ownership, financials, sanctions, or legal issues
- Immediately receive notifications of any supplier red flags
- Continuously update vendor risk profiles
- Enhanced analysis with data
- Screen suppliers against aggregated risk data covering millions of entities
- Use artificial intelligence to identify hidden network links and anomalies
- Uncover trends and emerging fraud typologies across the procurement ecosystem

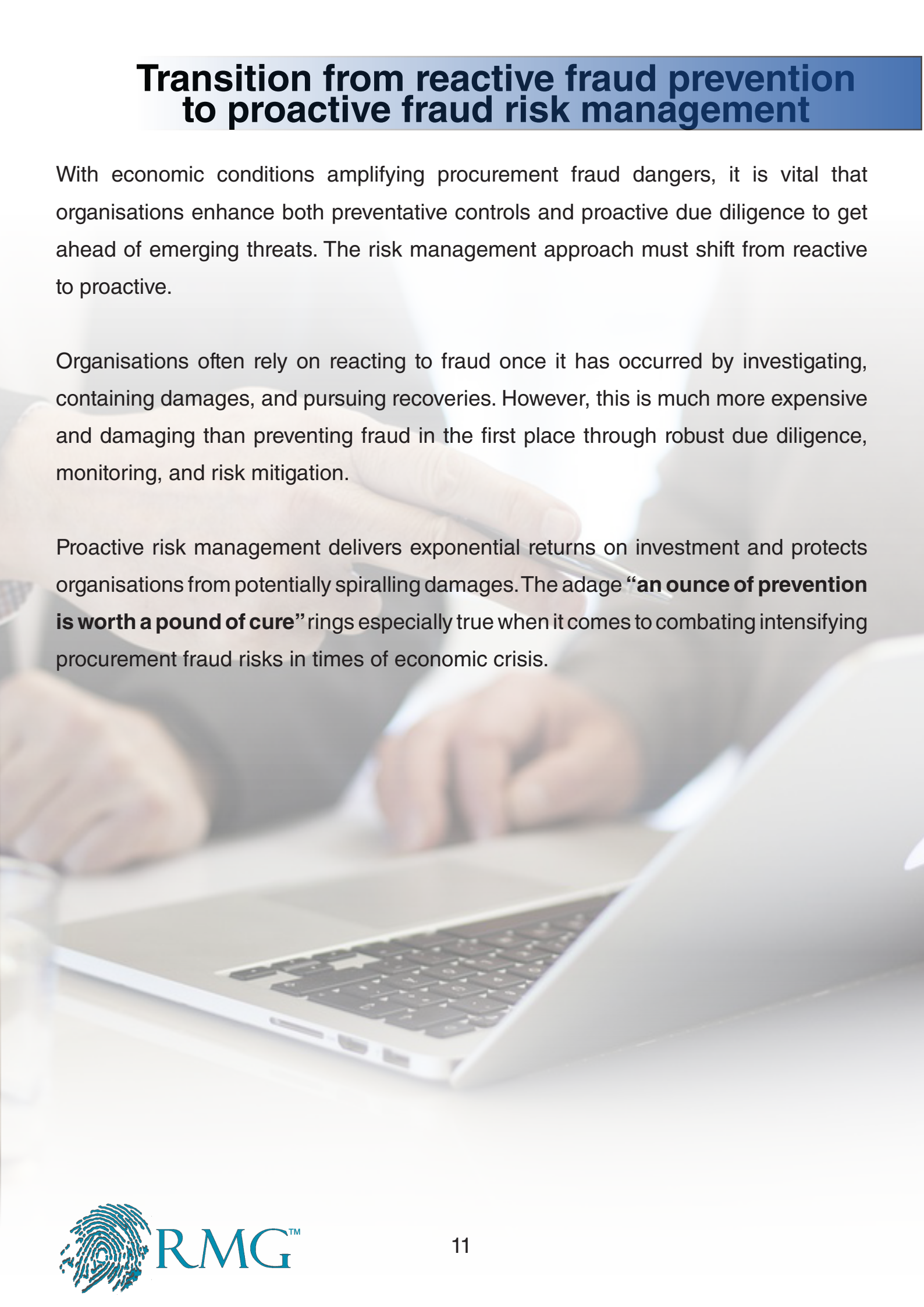
By harnessing scalable and intelligent technology, organisations can transform supplier due diligence into a formidable line of defence against intensifying procurement fraud risks.

Transition from reactive fraud prevention to proactive fraud risk management

With economic conditions amplifying procurement fraud dangers, it is vital that organisations enhance both preventative controls and proactive due diligence to get ahead of emerging threats. The risk management approach must shift from reactive to proactive.

Organisations often rely on reacting to fraud once it has occurred by investigating, containing damages, and pursuing recoveries. However, this is much more expensive and damaging than preventing fraud in the first place through robust due diligence, monitoring, and risk mitigation.

Proactive risk management delivers exponential returns on investment and protects organisations from potentially spiralling damages. The adage **"an ounce of prevention is worth a pound of cure"** rings especially true when it comes to combating intensifying procurement fraud risks in times of economic crisis.



A holistic commercial crime prevention approach at all levels of business

Implementing a holistic anti-fraud program:

Fraud and unethical behaviour pose serious risks that require a co-ordinated, organisation-wide approach to mitigate effectively. A robust anti-fraud program must have buy-in and commitment from senior leadership to signal the importance of integrity throughout the company in a top-to-bottom approach. Comprehensive policies need to be coupled with thorough training to ensure staff at all levels understand emerging fraud schemes and how to spot red flags. Ongoing vendor screening and auditing is critical to avoid compliance lapses.

The key takeaway is that preventing fraud and unethical conduct is not a one-time initiative, but an ongoing holistic commitment amongst business, vendors and service providers. A multi-layered approach covering policies, training, vendor oversight, and leadership commitment is essential in fostering an ethical culture and reducing fraud risk. Vigilance and co-ordinated effort across all facets of the organisation are imperative to protect against threats in an evolving risk landscape.