Deloitte.

Risk Angles
Five questions on white-collar crime

This issue of Risk Angles is focused on managing the risks of white-collar crime and the use of Big Data to proactively address fraud risks; ultimately allowing executives to focus on what must go right.

White-collar crime is a well-known and widespread problem that impacts brand value and reputation, goodwill, and profitability of many organisations; any one or a combination of these outcomes ultimately impacts stakeholder value. In addition to the risk of losses from white-collar crime itself, companies also face spiralling costs in related areas. Compliance with increasing regulation, ongoing crime detection efforts, internal investigations of potential wrongdoing, external enforcement actions and any associated fines and penalties, class action lawsuits, and other litigation are among the factors driving up both the costs and risks associated with white-collar crime. In order to effectively detect, assess, prevent and respond to white-collar crime, organisations need to consider a more strategic and holistic risk management approach.

Managed Forensic, developed by Deloitte based on actual experiences with clients' challenges across industries, allows organisations to comprehensively and robustly manage the risks of white-collar crime.

Managing the risks of white-collar crime

Question	Deloitte point of view
What do we mean by white-collar crime?	From fraud to electronic crime including intellectual property theft, money laundering to bribery and corruption, market abuse and insider dealing to sanctions — all of these forms of white-collar crime are on the rise and share a common denominator: money.
Why does white-collar crime pose a bigger threat today?	White-collar crime is an ever-present threat for organisations. The value of what criminals actually take is only part of the cost – add the likely costs of penalties, civil judgments, and the cost of litigation and conducting investigations and suddenly the actual loss to an organisation is significantly greater than originally anticipated. Bribery, fraud, and cybercrime are continually evolving and becoming increasingly sophisticated. Regulatory agencies demand more accountability and as business embraces globalisation, it encounters new cultural, regulatory and legal challenges; not to mention cultural practices within certain economies.
How are companies managing the risks associated with white-collar crime?	A fragmented approach is not enough and neither is an exclusively reactive one. In fact, this approach ultimately has a greater impact on the organisation in both monetary and non-monetary costs. Compliance-based approaches addressing particular risks in a siloed or piecemeal fashion are giving way to holistic approaches that look at many types of white-collar crime risk across the organisation. Regulators expect to see this risk-based approach, yet still expect an overall compliance strategy. Regulators are looking for someone such as a Chief Compliance Officer, Chief Risk Officer or Chief Legal Officer to have over-arching responsibility. Overall, the trend is toward a broader risk-based approach with shared responsibility and oversight by management, staff, the board of directors and

Question	Deloitte point of view
	internal audit. Accomplishing this transition typically involves a focused change management effort for the organisation.
Why do companies' compliance, anti-fraud, anti-money laundering, and similar programs fail?	Failure to prevent or detect issues is often not because the programs or controls themselves are lacking. More often, it's a failure of culture and a lack of effective change management. For example, senior leaders may not be setting a strong or consistent "tone at the top" about acceptable and unacceptable behaviours or failing to apply consistent sanctions to indiscretions by employees. Or perhaps there isn't enough attention paid to gaining buy-in from the lines of business for new policies or processes. Or staff training and awareness efforts may be lacking. The infrastructure to prevent white-collar crime may be sound, but its effectiveness still depends on execution, on individuals doing the right thing at the right time — culture is what enables and drives those appropriate behaviours.
What role does technology play in managing white-collar crime risk?	Technology tools can give organisations a more holistic view of their data, highlight potential areas of risk and allow them to be more focused or targeted in their efforts to combat white-collar crime. Advanced analytics may help companies be more predictive in identifying trends and patterns indicative of white-collar crime risk that are not otherwise easily discernible. Overall, the emphasis today is on prevention and/or early detection; leveraging technology and analytics to proactively identify issues or potential issues before they turn into front-page news.

A closer look: Using Big Data to proactively address fraud risk

"Big Data" has become a commonly used term to describe the explosion in the volume, variety and speed of information generated in the course of our daily lives. Big Data encompasses:

- **Traditional enterprise data** from customer information systems, ERP data, online transactions, financial data (general ledger, accounts payable, accounts receivable), fraud hotline data (Tip-offs Anonymous) and the like.
- **Machine- or sensor-generated data** from sources such as Call Detail Records (CDR), weblogs, smart meters, manufacturing sensors, equipment logs and trading system data.
- **Social data** from customer feedback streams, blogging sites and social media platforms.

Over the last 10 to 15 years, there has been a leap in the use of data analytics to mine Big Data to identify the patterns, trends, and anomalies that are often indicators of fraud or other types of white-collar crime. In the past, these have been siloed efforts in response to particular incidents or investigations. Now there appears to be a much broader effort to proactively detect, deter and prevent white-collar crimes. Big data and analytics are shaping how companies approach these efforts. For example, Enterprise Fraud and Misuse Management (EFM), is becoming more widespread as it allows organisations to integrate technology platforms, methodologies, and analytics approaches to proactively identify the indicators of fraud. EFM can provide a holistic, real-time or near real-time view of data to expose fraud risk across the organisation.

As an example, an organisation was faced with processing and analysing massive amounts of structured and unstructured data to continue its oversight and monitoring functions. Implementing an EFM infrastructure allowed it to explore the data efficiently, develop models, and then refine those models to predict and provide alerts about potential fraudulent behaviour. Case management was incorporated to manage alerts to resolution, and then those results were fed back into the models to identify positives and false positives in order to improve the models' effectiveness. Social network analysis was utilised to identify previously unknown relationships and expand the network of potentially fraudulent actors and activity.

Even with the advances in technology, many companies simply are trying to figure out where to start. They may be struggling with the amount of data and the daunting task of integrating and condensing it into manageable chunks. Deciding what to focus on and who should own the process are further sticking points. In many instances, it's helpful to take a pilot approach — choosing a particular type of white-collar crime risk (corruption, for example) or concentrating on a particular region. This can allow you to practice and refine data analysis techniques and methodologies, and see incremental progress, before implementing them on a broader scale.

For more information, contact:

Dave Kennedy
Managing Director, Risk Advisory, Africa
(Johannesburg)
Tel: +27 11 806 5340
Email: dkennedy@deloitte.co.za

Praveck Geeanpersadh
Africa Leader: Financial Crime
(Johannesburg)
Tel: +27 11 806 5437
Email: pgeeanpersadh@deloitte.co.za

Marc Anley
Director: Risk Advisory
Tel: +27 11 806 6052
Email: maanley@deloitte.co.za

Anthony Smith
Director: Risk Advisory
Tel: +27 11 209 8445
Email: asmith@deloitte.co.za

Navin Sing
Director: Risk Advisory
(Durban)
Tel: +27 31 560 7307
Email: navising@deloitte.co.za

Pramesh Bhana
Africa Leader: Governance, Risk and Oversight
(Johannesburg)
Tel: +27 11 806 5386
Email: pbhana@deloitte.co.za

Nina le Riche
Director: Risk Advisory
(Cape Town)
Tel: +27 21 427 5669
Email: nleriche@deloitte.co.za

Sisa Ntlango
Associate Director: Risk Advisory
(East London)
Tel: +27 43 783 4006
Email: sntlango@deloitte.co.za

Graham Dawes
Leader: Risk Advisory, Rest of Africa
(Nairobi)
Tel: +254 71 989 2209
Email: gdawes@deloitte.co.za