Shirley Ivason-Wagener

Partner
Country lead for fraud risk management
Tel: +27 82 714 0278
Email: shirley.ivason-wagener@kpmg.co.za

Eugine Sithole

Associate Director
Forensics
Tel: +27 60 985 4523
Email: eugine.sithole@kpmg.co.za

Article contribution recognition

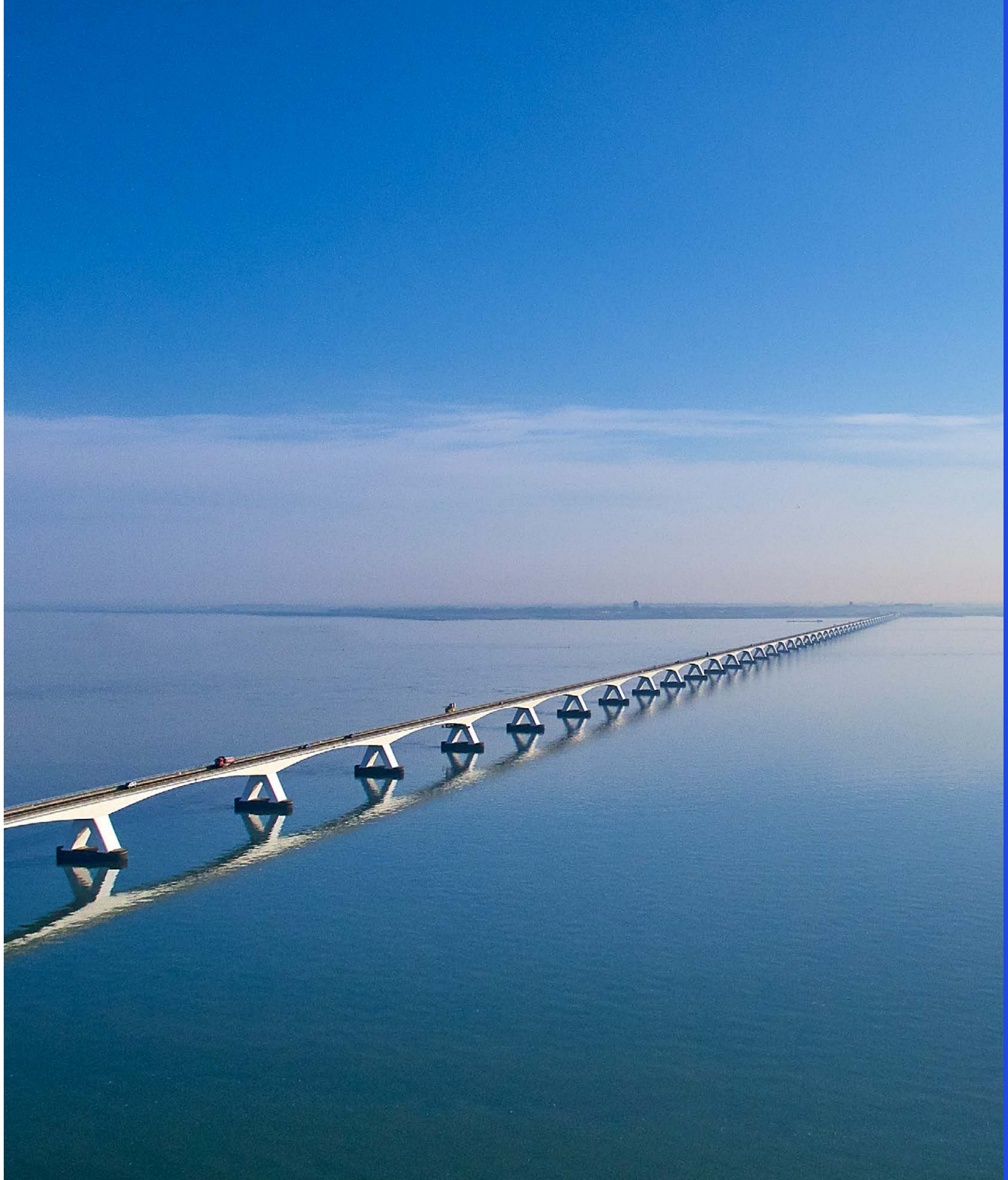
Joke Van Vuuren: Senior Manager (Forensics)
Nompilo Jele-Mpofu: Investigator (Forensics)

Mitigating insurance fraud risks

Introduction

Fraud in the insurance industry is on the rise due to a multitude of factors that create opportunities and incentives for fraudulent activities, including, but not limited to, financial instability, economic recessions, technology advancements, increased access to information and the pressure experienced by insurance agents and brokers to meet sales targets or earn commissions.

The insurance business lifecycle is highly prone to fraud which can lead to significant financial loss, reputational damage, regulatory penalties and operational disruptions.



While fraud in the insurance industry is not a new phenomenon, fraud is on the rise due to a multitude of factors that create opportunities and incentives for fraudulent activities. Some of the key reasons why fraud is increasing in the insurance industry include:

Economic downturns

Financial instability and economic recessions often lead individuals and businesses to commit fraud to gain financial relief. Economic stress can push otherwise honest individuals towards fraudulent activities to cover debts or maintain a certain lifestyle.

Technological advancements

While technology has streamlined many insurance processes, it has also provided fraudsters with new tools and methods to perpetrate fraud. Cybercriminals can exploit vulnerabilities in digital systems, manipulate data and create false identities more easily.

Complexity of insurance

The growing complexity and diversity of insurance products can create confusion among policyholders and provide opportunities for fraud. Misunderstandings about policy terms and coverage can lead to both opportunistic and deliberate fraud.

Weak regulatory oversight

Inconsistent regulations and lack of stringent enforcement can create environments where fraudulent activities are less likely to be detected or punished. Fraudsters may exploit these gaps to commit and get away with fraud.

Increase in organised crime

Organised crime groups are increasingly targeting the insurance industry due to the potential for high rewards. These groups often engage in sophisticated fraud schemes that are difficult to detect and combat.

Inadequate internal controls

Insurance companies may have insufficient internal controls and fraud detection mechanisms. This can be due to budget constraints, outdated technology, or lack of skilled personnel trained in fraud prevention.

Social and cultural factors

In some cultures, insurance fraud is perceived as a victimless crime or as a way to "beat the system." This social acceptance can encourage more people to engage in fraudulent activities.

Increased access to information

With more information available online, fraudsters can easily research and exploit specific vulnerabilities in insurance systems. This includes knowing how claims are processed and identifying weak spots in fraud detection systems.

Pressure to meet sales targets

Insurance agents and brokers under pressure to meet sales targets or earn commissions might resort to fraudulent activities, such as inflating claims or selling unnecessary to fake policies.

Addressing these factors requires a multifaceted approach, including better regulatory frameworks, advanced technology for fraud detection, improved internal controls, and public awareness campaigns to change cultural attitudes towards insurance fraud.

In this article we will discuss areas in an insurance business that are prone to fraud, the nature of the fraud risks and trends as well as navigate how insurance companies can mitigate the fraud risks.

Fraud in the insurance industry

Trends and statistics

The Association for Certified Fraud Examiners (ACFE) in its 'Occupational Fraud 2024: Report to the Nations'[1] concludes that corruption, payment tampering, and billing schemes are considered to be high-risk areas for insurance companies.

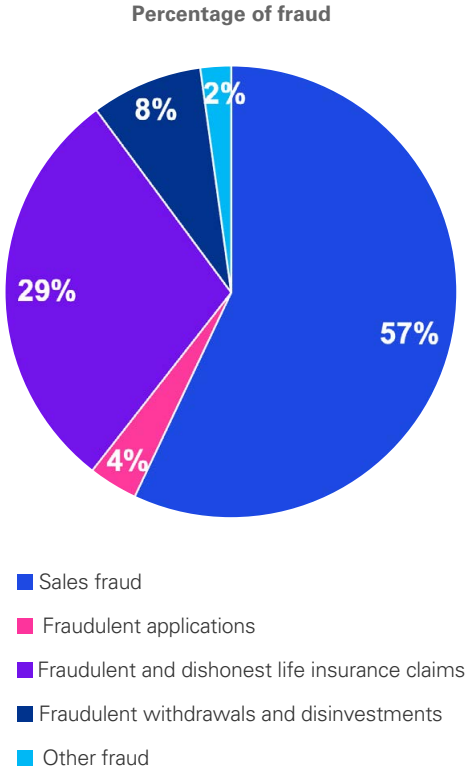
The ACFE study looked into the costs and effects of occupational (fraud committed by an organisation's employees) across eight regions namely; United States and Canada, Sub-Saharan Africa, Asia-Pacific, Southern Asia, Middle East and North Africa, Western Europe, Latin America and the Caribbean and Eastern Europe and Western/Central Asia. Of the total 1 921 fraud cases reported 299 (16%) cases were reported in Sub-Saharan Africa.

Of the 299 cases of reported fraud in Sub-Saharan Africa, 88 cases were reported in South Africa, the most in this region and across the whole of Africa. Specific to the insurance industry, ASISA provides further insights into the increasing cases of fraud.

The fraud statistics are divided into five categories as follows:

1. **Sales fraud:** fraudulent attempts by call centre agents, tied agents and independent financial advisers to benefit from commission/fees.
2. **Fraudulent applications:** misrepresentation, non-disclosure, impersonation, identity theft.
3. **Fraudulent and dishonest life insurance claims:** fraudulent and dishonest attempts to claim benefits from risk policies.
4. **Fraudulent withdrawals and disinvestments:** linked investment service providers, collective investment schemes, retirement funds.
5. **Other fraud:** fraudulent attempts to obtain investment policy benefits and bribery and corruption.

The graph below illustrates the percentage of fraud in each category:



From the ASISA fraud statistics, it is clear that sales fraud and fraud relating to life insurance claims are most prevalent in the insurance industry, making up 86% of reported instances in 2022.

[1] https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf

Areas prone to fraud in the lifecycle of an insurance business

Fraud can infiltrate every stage of the insurance business lifecycle, from product development and launch stage to post-settlement stage, affecting various processes along the way. Understanding the fraud prone areas helps insurers implement targeted strategies to prevent, detect and respond to fraud.

The illustration below depicts the insurance business lifecycle and the extent to which these areas are prone to fraud. The prevalence of fraud in the various areas is rated as high (red), medium (orange) or low (green) risk:

Fraud risks in the insurance industry are multifaceted and there are various types of fraud which can manifest throughout the insurance lifecycle. Potential fraud risks include, but are not limited to:

Identity fraud: fraudsters using stolen identities to apply for insurance cover and submit false claims.

Misrepresentation: a false statement of fact which renders other statements misleading. This false statement can be made knowingly, recklessly or innocently.

Fronting: using legitimate or innocent individuals or entities to conceal the true ownership, control, or involvement of another person or organisation.

Claims fraud: submission of fraudulent claims, exaggeration of losses, or stage accidents to receive undeserved pay-outs.

Premium diversion: the unauthorised use or misappropriation of insurance premiums paid by policyholders to agents, brokers or representatives.

Billing fraud: the intentional manipulation or falsification of invoices, bills or payment to deceive an organisation into paying/overpaying for goods or services that were not provided.

Internal fraud: the intentional acts by employees, agents or contractors within an organisation that results in financial or non-financial loss or reputational damage.

Healthcare and provider fraud: intentional acts of deception, concealment or misrepresentation by healthcare providers to obtain unauthorised financial gain or benefits.

Policyholder fraud: the intentional acts of deception, concealment or misrepresentation by a policyholder or beneficiary to obtain unauthorised benefits, discounts or advantages.

Extortion: the unlawful attainment of money, property or services from another through coercion, threats or intimidation.

Reinsurance fraud: involves deceptive practice of one insurance company transferring a portion of its risks to another to reduce potential losses.

Disaster fraud schemes: an intentional deception to defraud individuals and the government that results in personal gain, e.g. charitable solicitation, contractual fraud, price gouging and insurance fraud.

Blackmail: the act of threatening to reveal sensitive, damaging or embarrassing information unless a person complies with certain demands involving payment, favours or compensation.

Agent fraud: refers to intentional acts of deception by agents including lapping, skimming, creating fictitious policies, forgery and churning.

Application fraud: individuals provide false or misleading information on an application with the intent to deceive the insurer and obtain coverage under false pretences.

Underwriting fraud: misrepresentation of risks during underwriting which can lead to under-priced policies.

Social engineering: a technique used by fraudsters to gain access to confidential information through manipulation. Deception fraudsters convince victims to perform actions or divulge confidential information.

Commission fraud: agents inflating their commission by engaging in fraudulent activities.

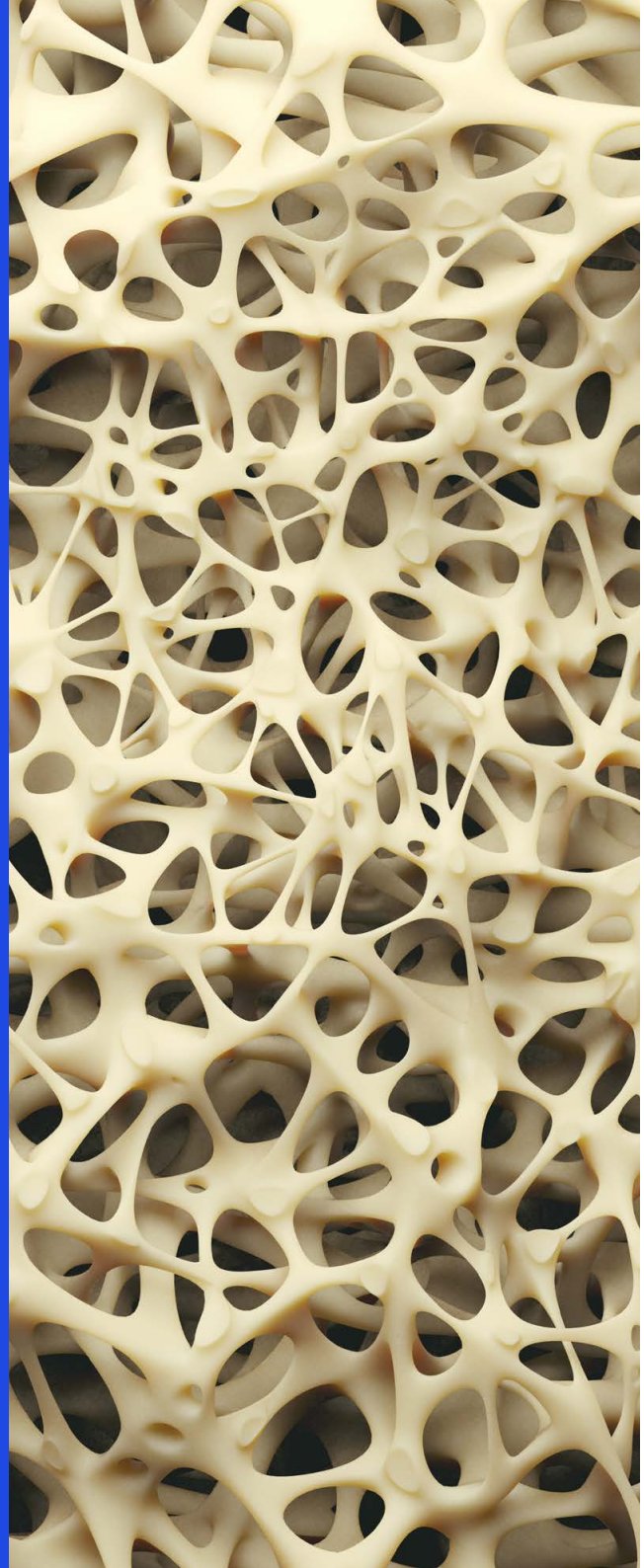
Secret commissions: unauthorised and concealed payments or receipt of commissions or favours to the agents without the knowledge of the principal.

Bribery: a form of corruption, including anything of value, such as cash, gifts, or control of proceeds from financial crimes, making them seem legitimate.

Money laundering: concealment of the origins or source of illicit funds obtained through criminal activities by integrating them into legitimate insurance transactions.

Abuse of company facilities: unauthorised, improper or excessive use of an organisation's resources, assets or services for personal gain, benefit or convenience.

Deliberately omitting or refusing to report or act upon reports of any such irregular or dishonest conduct.



Mitigating the fraud risks

Due to the dynamic nature of fraud, it is imperative for insurance businesses to make strides towards implementing mature Fraud Risk Management Frameworks with adequate preventative and detective measures.

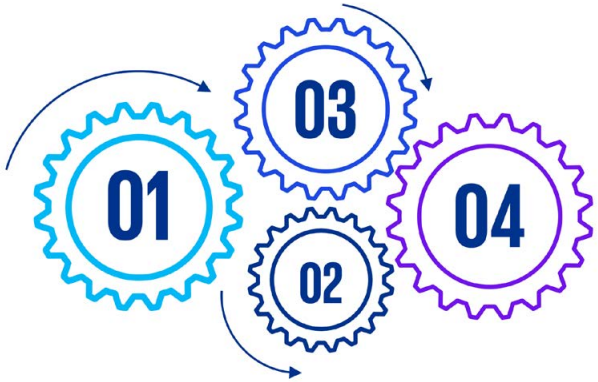
Below is an illustration of what a mature Fraud Risk Management Framework encompasses:

Set up a fraud monitoring framework

Develop and implement underlying system architecture leveraging artificial intelligence and machine learning.

Design fraud risk governance and operating framework

- Develop anti-fraud policies, procedures and applicable guidelines.
- Identification and assessment of emerging fraud risks.



Adequate and timely reporting

Based on the early warning signals, triggers and fraud alert reports are generated and circulated to concerned stakeholders at different time intervals ranging from near real-time to annual periodicity.

Identify fraud scenarios

- Identify fraud scenarios and categorise scenarios.
- Link fraud scenarios to overall business strategy for risk based thresholds/appetites.

A mature Fraud Risk Management Framework makes use of the following technical enablers:

Data warehouse

A centralised repository that stores and manages large amounts of data from various sources, including transactional data, customer information and external data sources. Data warehouses enable efficient data analysis, pattern recognition, reporting and business intelligence.

Interactive dashboards

Visual representations of data that provide real-time insights into fraud risk indicators, metrics and KPIs. Interactive dashboards allow users to explore data, identify trends, anomalies, suspicious activities and drill down into specific areas of concern.

Fraud alerts

Automated notifications triggered by suspicious activity or anomalies detected by the fraud detection system or predefined criteria. Fraud alerts enable timely investigation and response to potential fraud.

Risk scoring system

A scoring model that assigns a risk score to customers, transactions or activities based on factors such as behaviour, demographics and transaction history. Risk scoring helps prioritise investigations and focus on high-risk areas.

Integration with external industry-wide repository

Collaboration with external data sources, such as:

- Fraud databases (e.g. Fraud Prevention Service)
- Industry-specific repositories (e.g. credit union or bank networks)
- Public datasets (e.g. government records, public databases)

This integration enables access to shared intelligence, best practices and aggregated data to enhance fraud detection and prevention.

In addition to the above, combating insurance fraud requires co-operation between insurance companies, law enforcement and regulatory bodies and employing advanced technologies like artificial intelligence for fraud detection e.g. SAS.

KPMG business case on using SAS - a strategic plan for financial crime

Set out in the image below is our view of a best practice financial crime strategic plan which will assist towards the implementation of an effective Fraud or Financial Crime Intelligence Unit (FCIU) within a claims department or compliance function, that has strong capabilities for investigations and a holistic view over global financial crime risk.

We have also identified certain key observation which contribute to a robust strategic plan and operating functionality, which includes, but is not limited to:

- the establishment and development of various modular and investigation capabilities such as custom-made financial crime investigation solutions, custom-made anti-financial crime dashboards, a fraud risk management solution, and fraud risk assessment, reporting and transaction monitoring; and
- the solutions above being overlayed and powered by the use of machine learning capabilities, statistical anomaly detection and interactive network analysis.

1. Modelling and optimisation

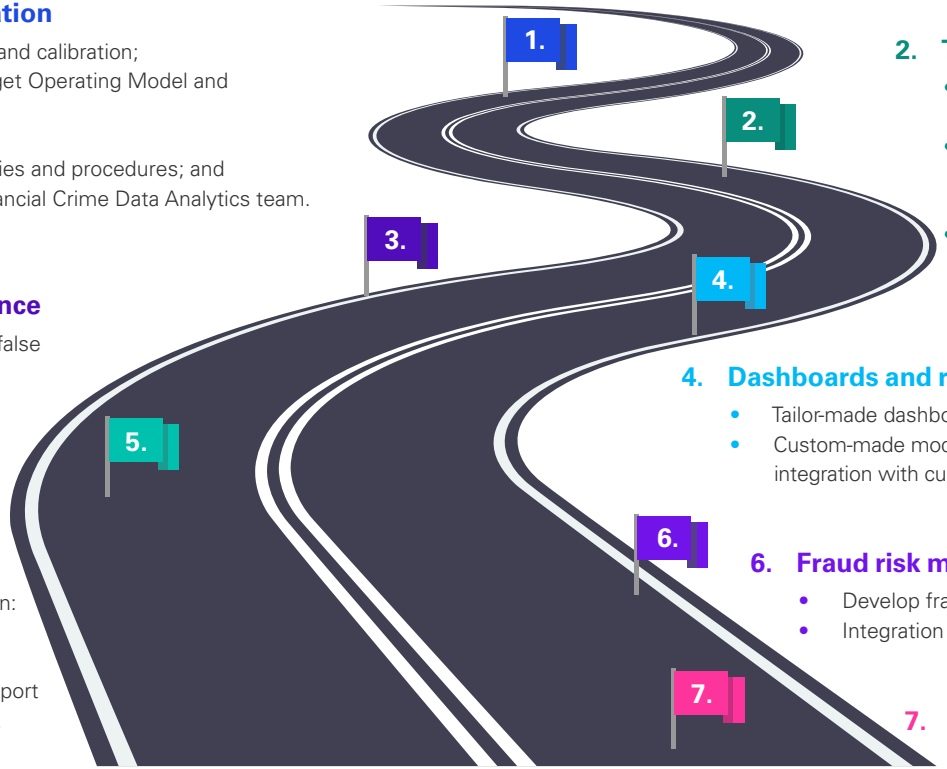
- Deep-dive system review and calibration;
- Financial Crime Global Target Operating Model and risk assessment;
- Remediation initiatives;
- Updating group-wide policies and procedures; and
- Creation of an internal Financial Crime Data Analytics team.

2. Transaction monitoring

- Online integration between KYC and onboarding;
- Supporting the organisation to develop rules into the onboarding platform (for each business line); and
- Implementation of the transaction monitoring solution with various scenarios and segments, overlayed with custom-made rules.

3. Machine learning and artificial intelligence

- Machine learning use cases (e.g.: reduction of false positives, detecting new patterns);
- Deep-dive calibration of the scenarios and clustering; and
- Automation of non-value operations and work.



4. Dashboards and risk assessment monitoring

- Tailor-made dashboards for operations, risk and calibration; and
- Custom-made module for developing yearly risk assessments and integration with customer due diligence and transaction monitoring.

5. Corporate intelligence unit

- Integrating several systems into the new solution: fraud, claims, underwriting etc.;
- Holistic and cross-border investigations; and
- Development of a custom-made system to support internal and external reports and investigations.

6. Fraud risk management

- Develop fraud batch scenarios; and
- Integration of investigation and fraud risk management.

7. Real time screening (ongoing)

- Real time customer and transactions screening.

KPMG

Conclusion

Insurance businesses need to invest in fostering ethical cultures, promote training and awareness programs and implement adequate measures to prevent fraud, bribery and corruption.

With the amendment of section 34 of the Prevention and Combatting of Corrupt Activities Act (PRECCA) the failure to prevent such activities has now been criminalised. Private entities, like insurance companies, now have the obligation to implement adequate prevention measures. However, no crime will be committed where a private-sector organisation or incorporated state-owned entity has put in place adequate prevention measures to stop anyone connected to the private-sector organisation or incorporated state-owned entity from agreeing to provide, providing, or offering to provide any gratification that is prohibited under Chapter 2 of the PRECCA. Failing to implement and prove that these measures have been implemented will find insurance companies liable in terms of PRECCA.

Therefore, implementation of appropriate prevention measures is now a necessity and no longer a “nice to have”. Insurance companies should be geared up for insurance fraud and ensure that its procedures are ‘adequate’ to prevent corruption and be in a defendable position.