



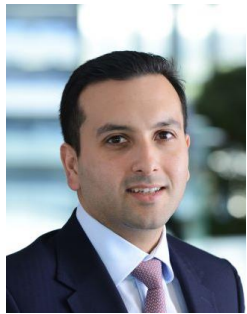
Fraud Awareness for Internal Auditors

The impact of Covid-19 on Fraud Trends

16 June 2020



Introduction presenters



Kami Zargar

Head of Forensic

kamizargar@kpmg.com



Jens Moerman

Manager Forensic

jensmoerman@kpmg.com



Wouter Monten

Senior Forensic Expert

wmonten@kpmg.com



Who joined us today?



Absa

Alcopa Group

AquaFlanders

Barco NV

Befimmo SA

Belchim Crop Protection NV

Carmeuse

Colruyt Group Services

Daikin Europe

De Vlaamse Waterweg

Dover Corporation

Duvel Moortgat

D ieteren

Fluvius

Federal Internal Audit

Greenyard

Holcim

Hulpkas voor Ziekte- en
Invaliditeitsverzekering

Kinopolis Group NV

Jan De Nul

MBAPL

NN Belgium

Rijksdienst voor Sociale Zekerheid

Pemda Kabupaten Bandung

Promethera Biosciences

Samsonite

Saudi Payments

SAS

SCR Sibelco

Total Raffinaderij Antwerpen

UCB

UGent

UZA

Vandemoortele

Willemen groep

ZNA

ZyLAB



The Current Covid-19 Climate

On the rise:



Demand for goods



Demand for information



Mobility & remote working



Economic uncertainty



Leading to:

Significant changes in business and working patterns

Significant economic impact on the performance of business

Unprecedented volume of cyber-attacks and cyber enabled fraud

Damage to employee wellbeing and customer sentiment

Today's agenda



Overview



1. Fraud: what is it and why do people commit it?

2. Covid-19 Trends

3. Fraud Prevention

4. In the event of a Fraud

5. Takeaways



Fraud:
what is it and why do
people commit it?

Categories of fraud

Misappropriation of assets

- Payroll fraud
- Expenses fraud
- Procurement fraud
- Theft of assets e.g. stock and cash
- Theft of intellectual property

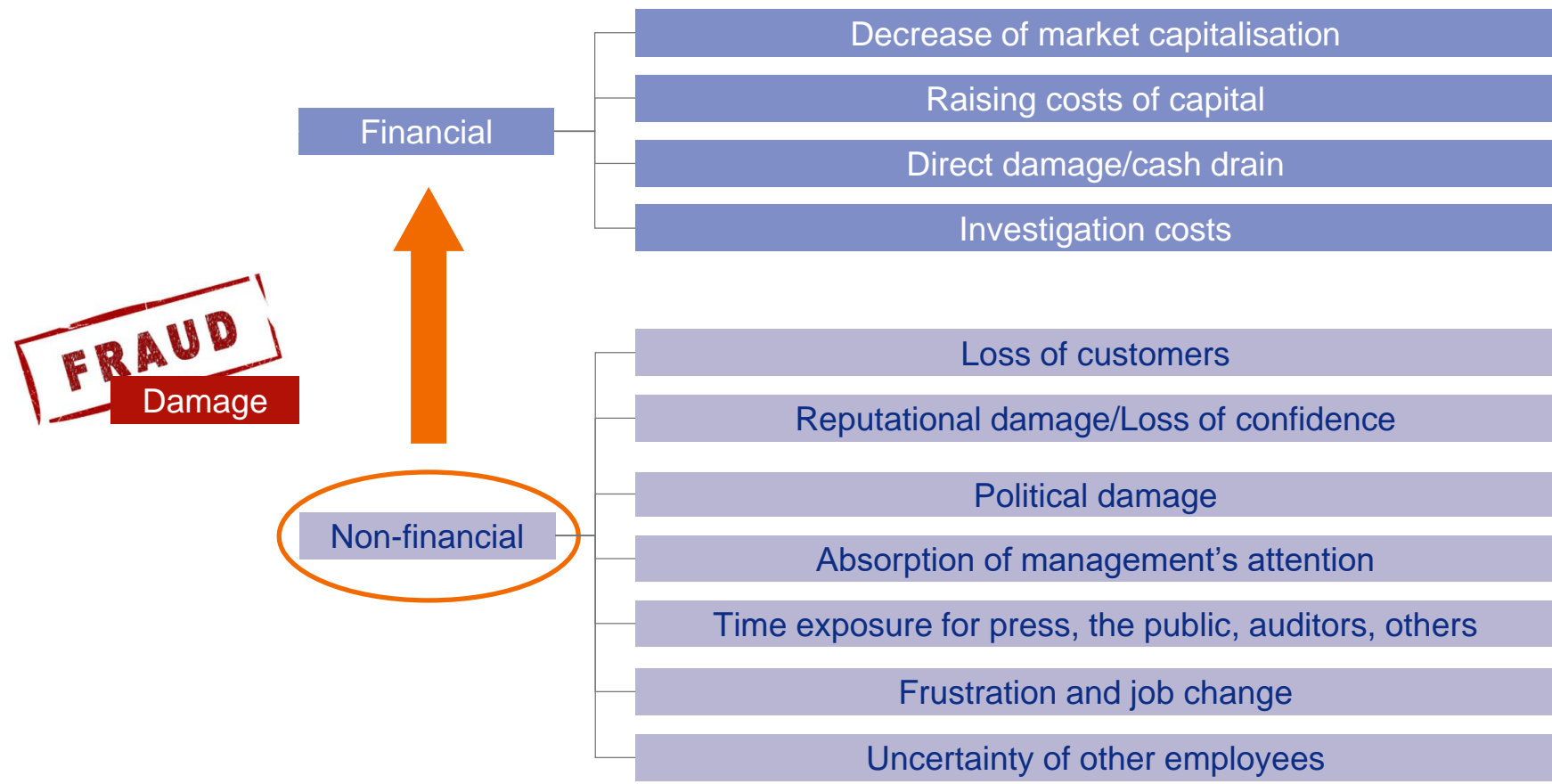
Fraudulent financial reporting

- Improper revenue recognition
- Overstatement of assets
- Understatement of liabilities
- Customer overbilling
- Treasury & investment related fraud

Related illegal activity

- Competitive behaviour
- Bribery and corruption
- Money laundering
- Organised crime
- Insider trading

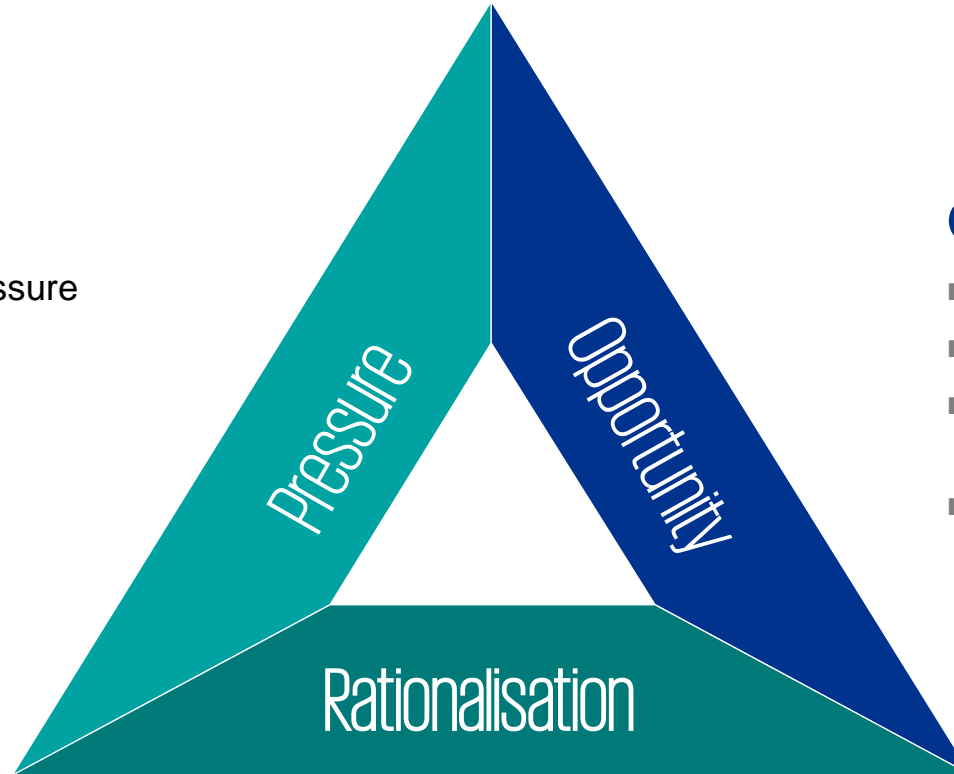
What is the impact of fraud?



Why do people commit fraud - the Fraud Triangle

Pressure

- Financial pressure
- Greed
- Addictions
- Revenge
- Desperation



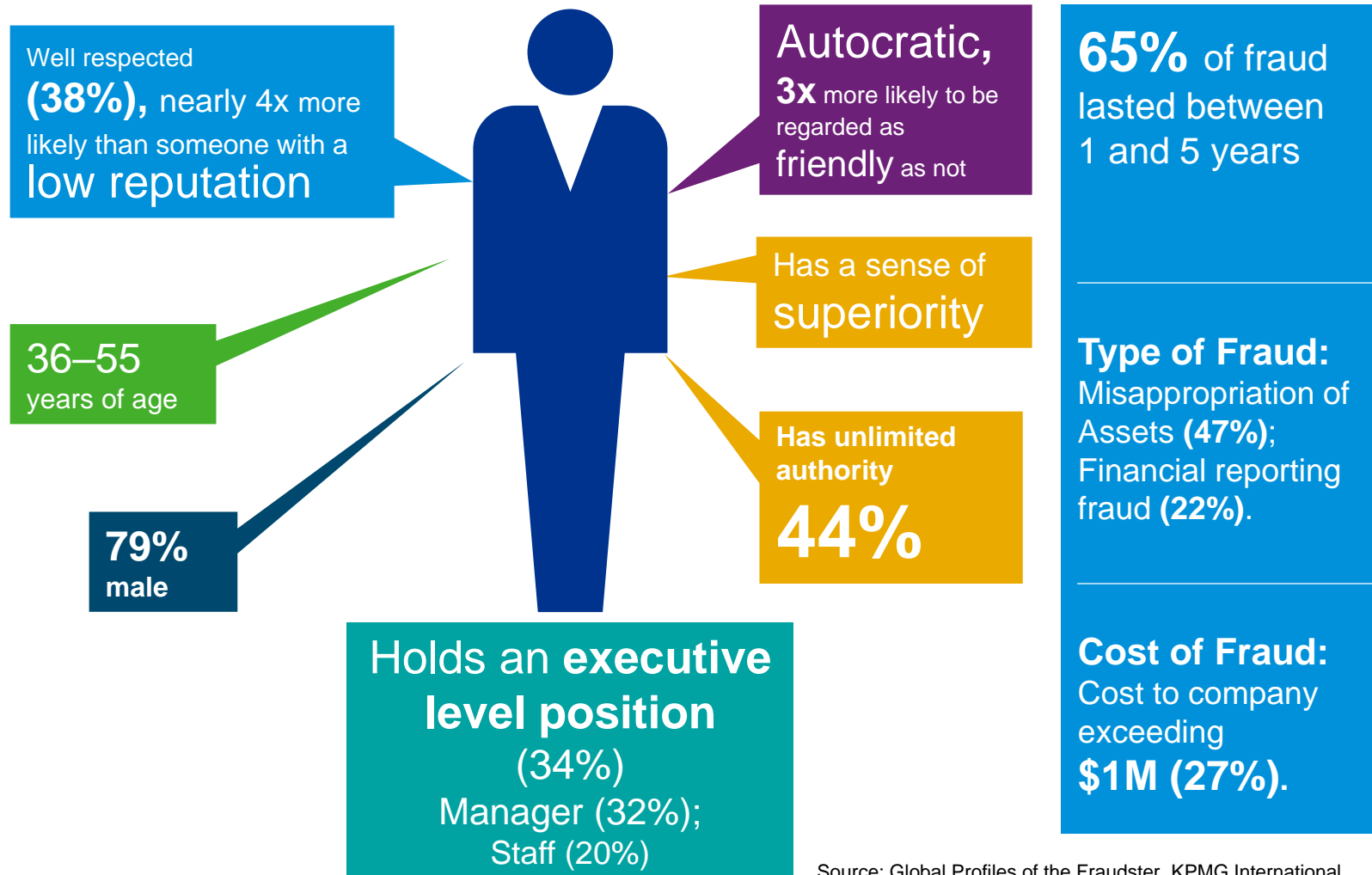
Opportunity

- Poor controls
- Abuse of authority
- Poor segregation of duties
- Exploiting errors

Rationalisation

- "I need the money"
- "I deserve more"
- "People need me to"

Fundamental characteristics: Overview

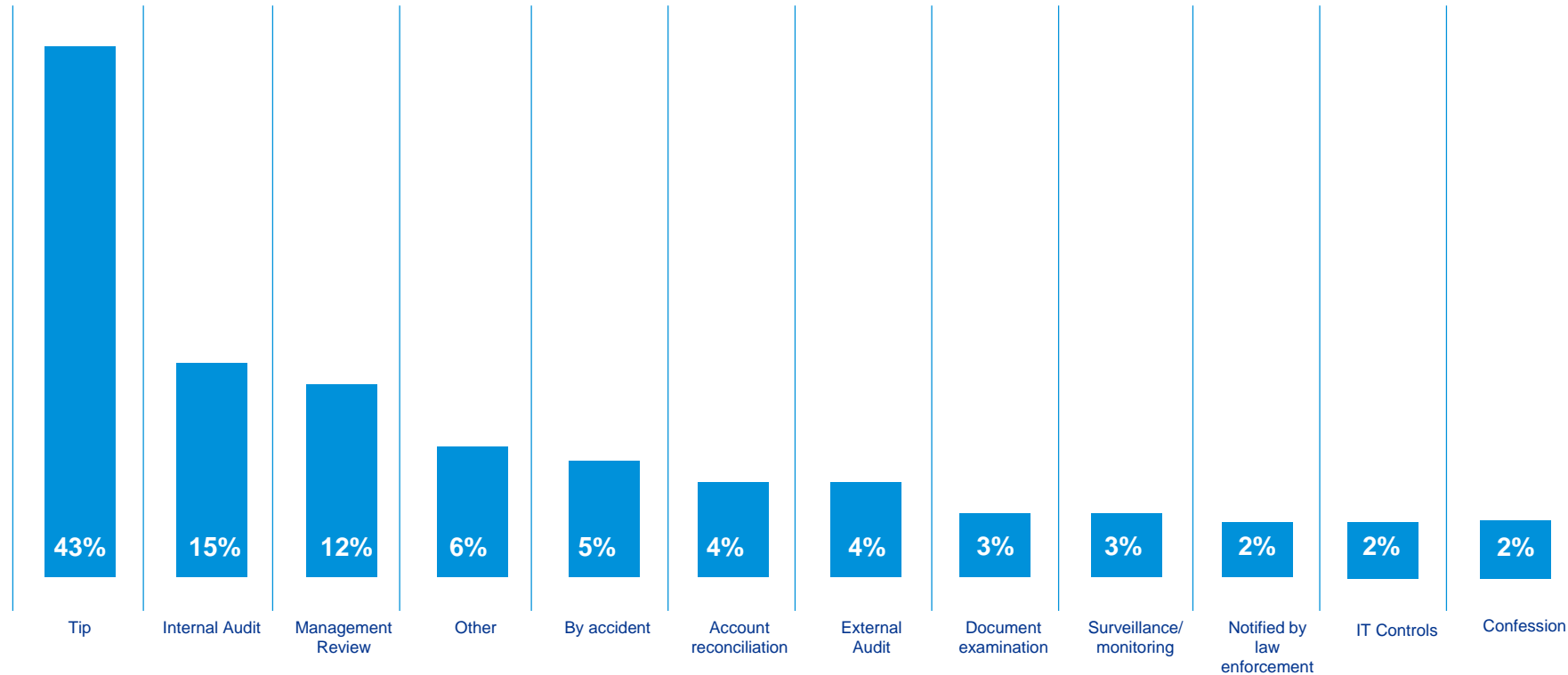


Organisational findings: fraud enablers



Means of detection

How were the Frauds detected?



Source: ACFE Report to the Nations 2020

New EU Directive on Whistleblower Protection coming into effect December 2021



Purpose:

To enhance enforcement of Union law and policies in specific areas by laying down common minimum standards providing for a high level of protection of persons reporting breaches

Obligation to have internal whistleblowing policies in private and public sector

For legal entities in private sector:

- 50 or more workers; or,
- Private companies active in financial services, products and markets, and AML and terrorist financing

Protection of whistleblowers:

- If reasonable grounds to believe that information was true at the time of reporting and within the scope of Directive
- Reported internally, externally or made public

Personal scope of application:

Protection of employees, persons with self-employed status, persons belonging to administrative management or supervisory body, volunteers and paid/unpaid trainees

Cascade system:

1. Internal reporting system (article 7) encouraged by member states
2. External reporting system (article 10)
3. Public disclosure (article 15)

Penalties:

Member States shall provide for effective penalties to natural or legal persons that:

- a) Hinder or attempt to hinder reporting
- b) Retaliate against reporting persons
- c) Bring vexatious proceeding against reporting persons
- d) Breach duty to maintain confidential the identity of reporting persons

Be on the lookout for our upcoming online self-assessment tool to gauge your organisation's maturity in terms of whistleblower protection and reporting!

For more detailed information on the Directive, please follow the following link:

<https://home.kpmg/be/en/home/insights/2019/12/rc-whistleblower-protection.html>



Covid-19 Trends

COVID-19 fraud examples

Belgium

Belgian authorities fear they may have fallen victim to a coronavirus scam - after an order of 5 million protective masks failed to turn up.

Belgium had joined several European neighbours in a group purchase for protective gear from a Turkish company.

Belgium

The Flemish government is claiming back €10 million as a result of corona premium related fraud.

According to figures from Flemish Minister of Work Hilde Crevits (CD&V). Government support has been provided for companies that have been hit hardest by the corona pandemic. In practice, however, it appears that companies that suffer little damage also applied for the aid.

Belgium

Fraudulent investments are being offered increasingly, in diverse forms and in very different domains.

These very diverse investments often hide the same fraudulent principle: the trust of a potential investor is won by a well-considered argument, a confident contact person and a professional-looking online platform where he can track his investment in real time. However, as soon as he wants to recover his stake or claim his winnings, all communication is cut and the scammers disappear with his money.

Netherlands

Dutch police took 10 fake web shops offline after they offered products such as COVID-19 tracker apps and anti-bacterial credit cards. Some had cloned the identities of legitimate shops.

France

A French school of engineering's name was used, without their consent, to certify the conformity of masks.

After being informed by a Italian pharmacist and an Hungarian company they discover the fraud and enforced legal actions.....

Spain

The Spanish government had to return 9,000 ineffective COVID-19 testing kits after buying them from an unauthorised and unlicensed company in China.

Switzerland

The Reporting and Analysis Centre for Information Assurance has detected large numbers of phishing and ransomware attempts linked to COVID-19. Some are sent in the name of the Federal Office for Public Health.

In addition, in March 2020 fishing attack was orchestrated against World Health Organization in which the fraudsters impersonated WHO to steal Bitcoin Covid-19 donations originally collected for the WHO's COVID-19 Solidarity Response Fund.

UK / Germany / Turkey

During the mayhem caused by the pandemic, companies around the world placed orders to acquire masks from all available sources; and it turned out that the supply never existed.

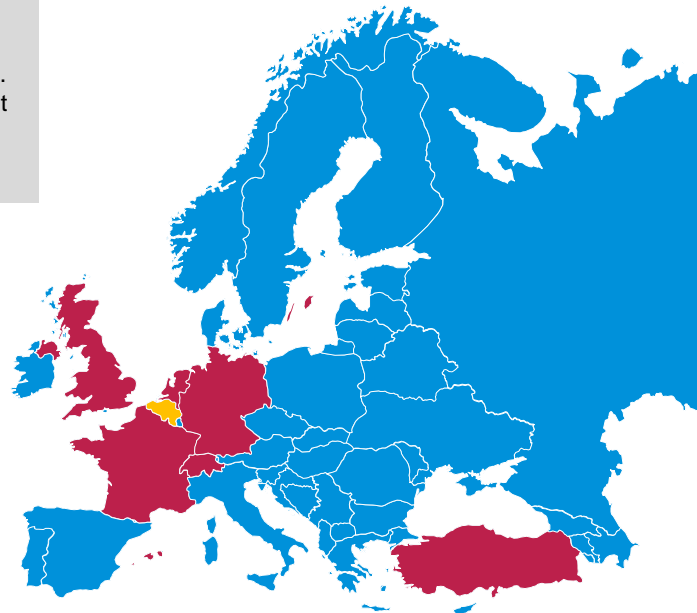
Fraudsters disappeared after obtaining a prepayment leaving companies with over EUR 20m in losses...

Italy

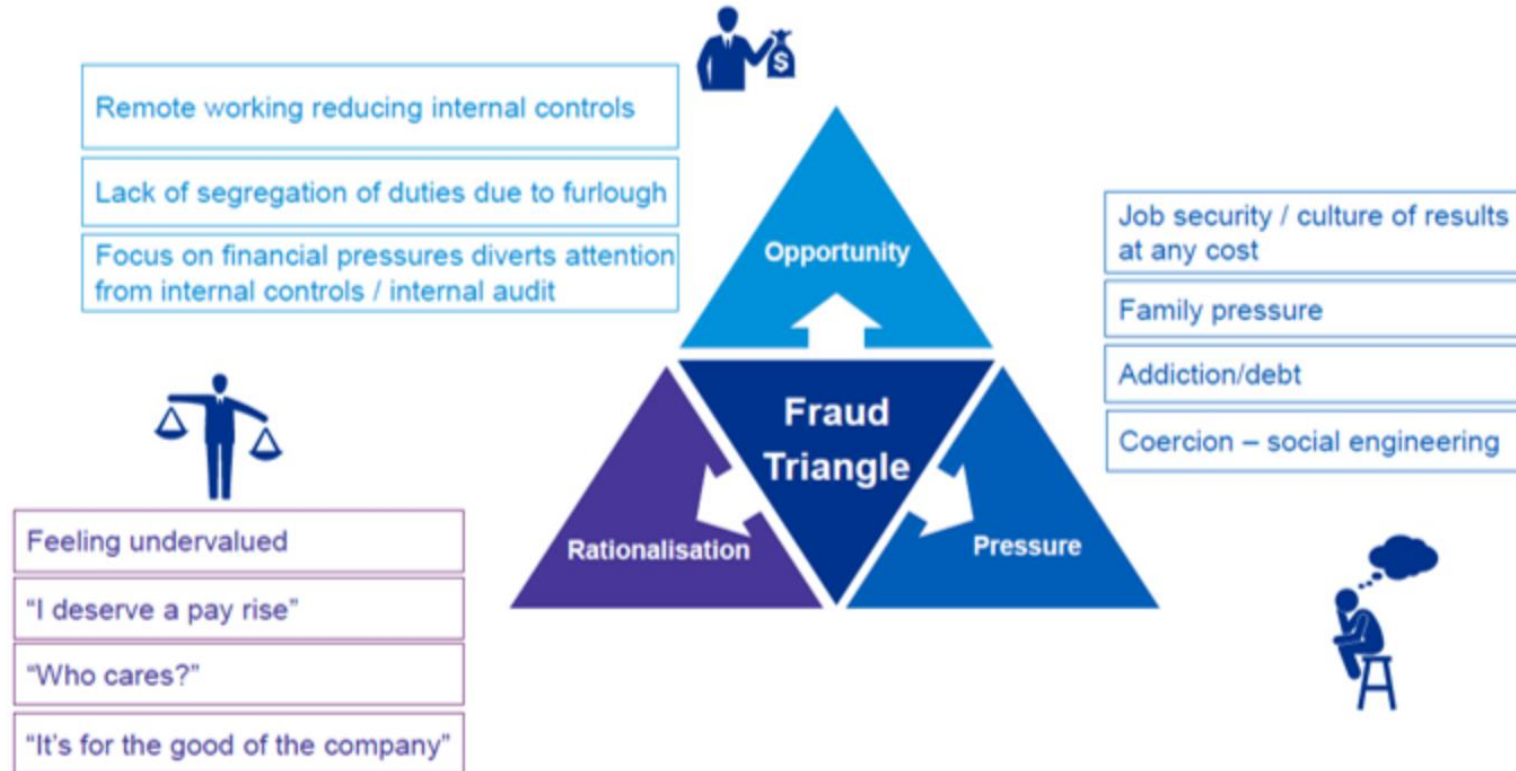
False declarations have been made to obtain government grants intended to support businesses during the pandemic.

Police have warned that people knocking on doors claiming to be testing for Coronavirus are actually seeking to steal valuables from the elderly.

Criminal organisations are thought to be taking advantage of the crisis to infiltrate vulnerable sectors of the economy such as through buying hotels.



The pandemic has contributed to the Fraud Triangle



Fraud alert



Economic downturn has created financial reporting pressure



Corporates should recognise the risk of management override of controls

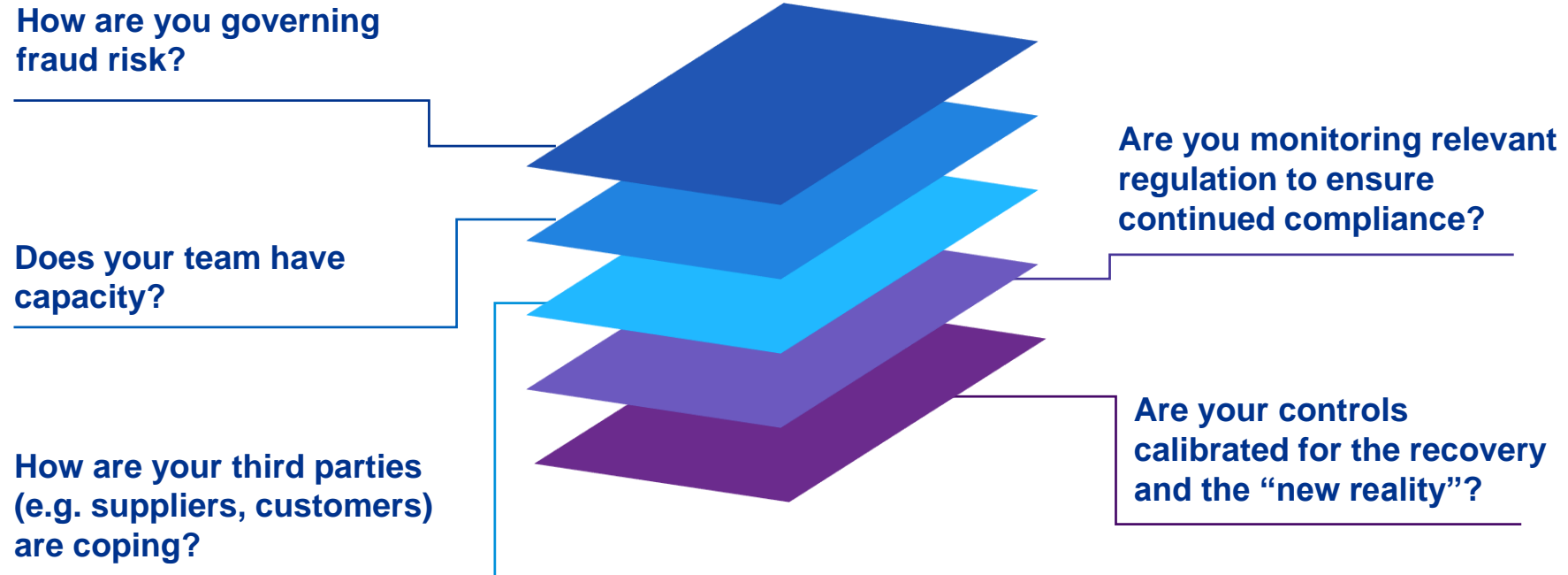


Individual pressures can increase traditional fraud risk areas of supply chain and procurement



Potential misuse of government aid schemes such as technical unemployment

Are you fraud control ready?

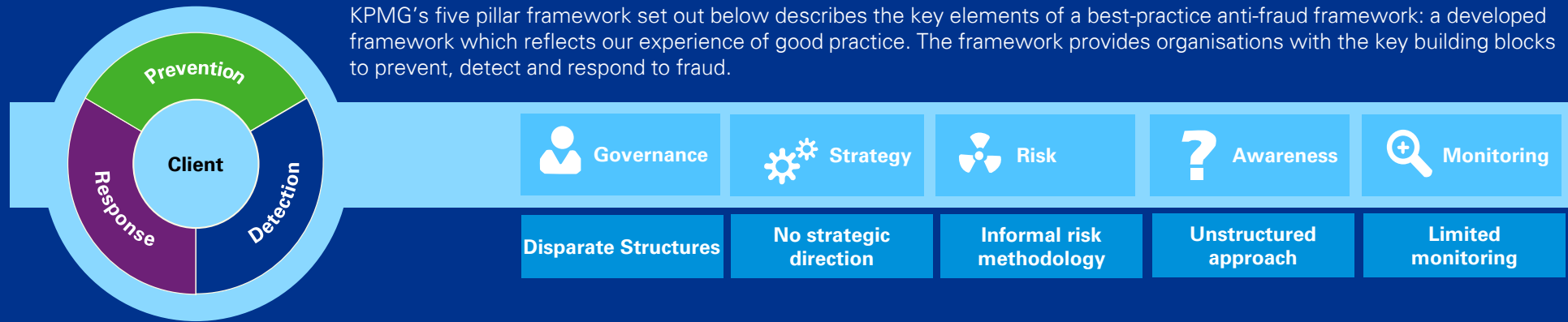




Fraud prevention



KPMG's Fraud Risk Management Framework



KPMG's five pillar framework set out below describes the key elements of a best-practice anti-fraud framework: a developed framework which reflects our experience of good practice. The framework provides organisations with the key building blocks to prevent, detect and respond to fraud.

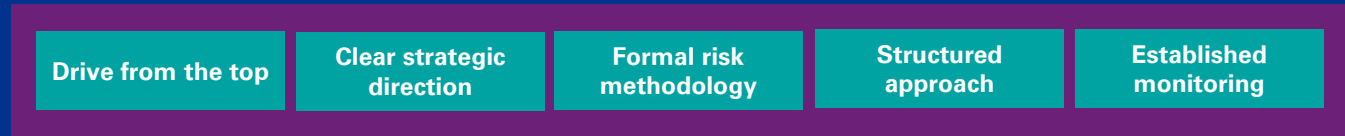
The framework aims to achieve three core objectives:

Prevent instances of fraud and misconduct from occurring in the first place.

Detect instances when they do occur.

Respond appropriately and take corrective action when instances arise.

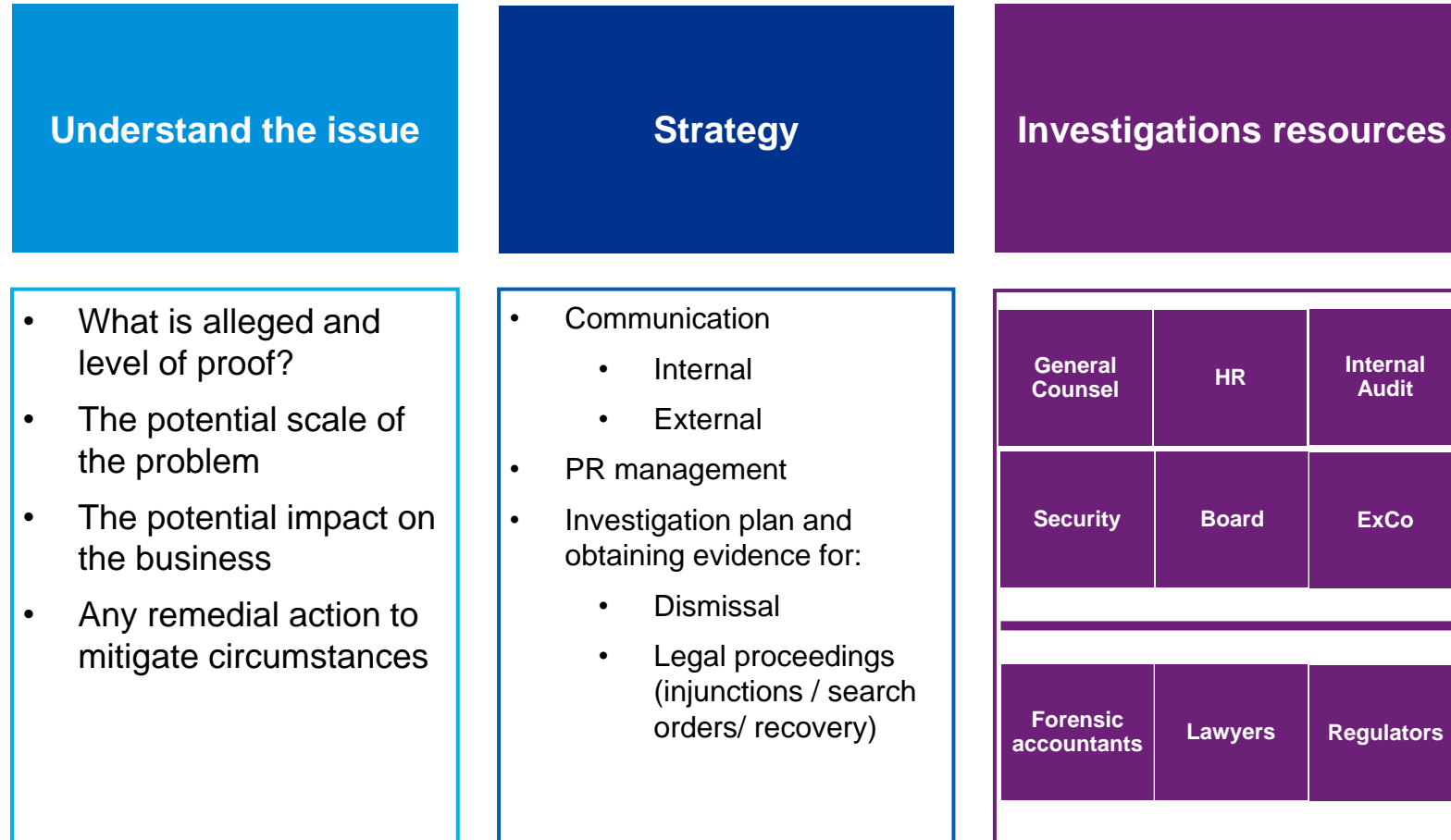
These three objectives run through all the five pillars of an effective anti-fraud framework.





In the event of a fraud

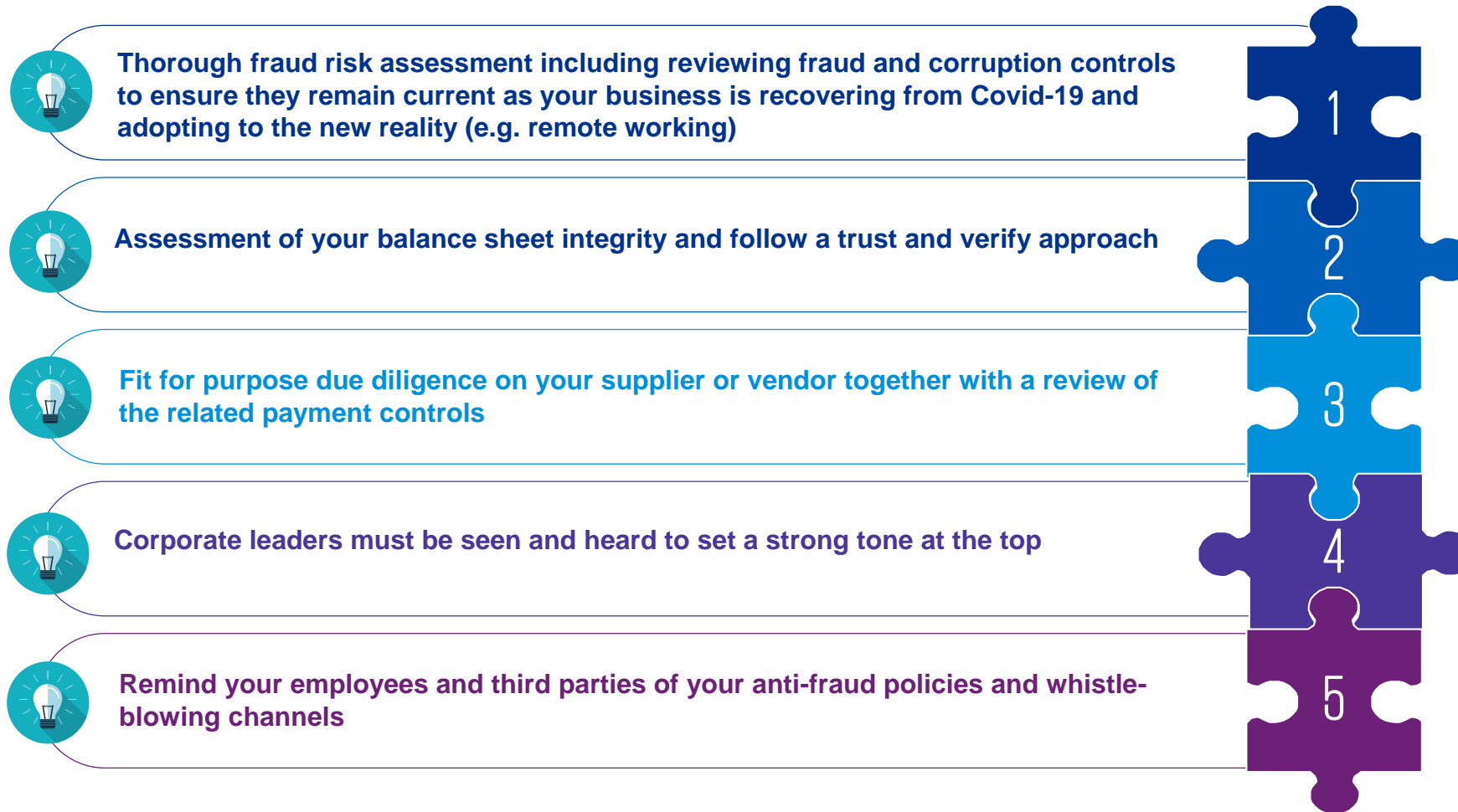
In the event of a fraud





Takeaways

Five take always to address fraud risk in the time of crises



Question and discussion



Kami Zargar

Head of Forensic

kamizargar@kpmg.com



Jens Moerman

Manager Forensic

jensmoerman@kpmg.com



Wouter Monten

Senior Forensic Expert

wmonten@kpmg.com





Thank you

Next webinar :

Effectively improve cyber resilience and drive automated compliance and risk management

17 June 2020 at 14.00pm



kpmg.com/be/social



kpmg.com/app

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

©2020 KPMG Advisory, a Belgian CVBA/SCRL and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.