Failing to prevent fraud

Avoiding corporate criminal liability

Building a better working world

The new era of corporate accountability for fraud

Large organisations now risk facing criminal prosecution and unlimited fines if they fail to prevent fraud. The Economic Crime and Corporate Transparency Bill 2022 ("the Bill") legislates a new corporate criminal offence of failing to prevent fraud[1] which, combined with changes to the law that applies criminal liability to corporates[2], will hold organisations accountable for the management of fraud risks across their organisation.

As the Bill has now received Royal Assent, it is expected that this new offence will be effective by the end of 2024, following publication of government guidance.

The legislation means that organisations will need to act now to understand their fraud risk exposure and develop an effective framework to help to prevent, detect and respond to the identified fraud risks.

In this article, we will share our insights into the key areas where we often see organisations struggle when trying to implement an effective fraud risk management programme.

ACFE estimates that organisations lose

5% of revenue to fraud each year, amounting to an estimated

$4.7 trillion global loss

in 2021.[3]

1. Factsheet: failure to prevent fraud offence – GOV.UK (www.gov.uk)
2. Factsheet: failure to prevent fraud offence – GOV.UK (www.gov.uk)
3. ACFE: Report to the Nations (www.acfe.com)

What are the new requirements?

The new corporate criminal offence of failure to prevent fraud has been implemented by the government to hold organisations to account if they benefit from fraud committed by their employees and agents.

What is the offence?

Under the new offence, an organisation will be liable where a specified fraud offence is committed by an associated person, for the organisation's direct or in-direct benefit, and the organisation did not have reasonable fraud prevention procedures in place. It does not need to be demonstrated that company directors ordered or knew about the fraud.

This offence will only apply to 'large organisations' meeting two out of three of the following criteria: more than 250 employees, more than £36 million turnover and more than £18 million in total assets.

Who are associated persons?

A person is associated with an organisation is an employee, third party, or subsidiary of the organisation, or the person otherwise performs services for or on behalf of the organisation.

What is a specified fraud offence?

Offences in scope are wide and detailed in the Bill but can be summarised as more simply as fraud committed by the organisation.

Examples of fraud by the organisation:

- Financial statement fraud, e.g., under recognising accruals
- Non-financial statement fraud, e.g., misreporting carbon emissions
- Rogue trading
- Corruption, including bribery
- IP theft

It will not be an offence if the organisation was, or was intended to be, a victim of the fraud.

What is the extra-territorial effect?

The Government's factsheet on the new offence states that 'if an employee commits fraud under UK law, or targeting UK victims, the employer could be prosecuted, even if the organisation (and the employee) are based overseas'.

What defence is available?

The only defence available to an organisation will be that of reasonable procedures at the time the fraud offence was committed. Guidelines will likely mirror those published by the Ministry of Justice regarding adequate procedure for the failure to prevent bribery offence.

When do I need to have reasonable procedures in place by?

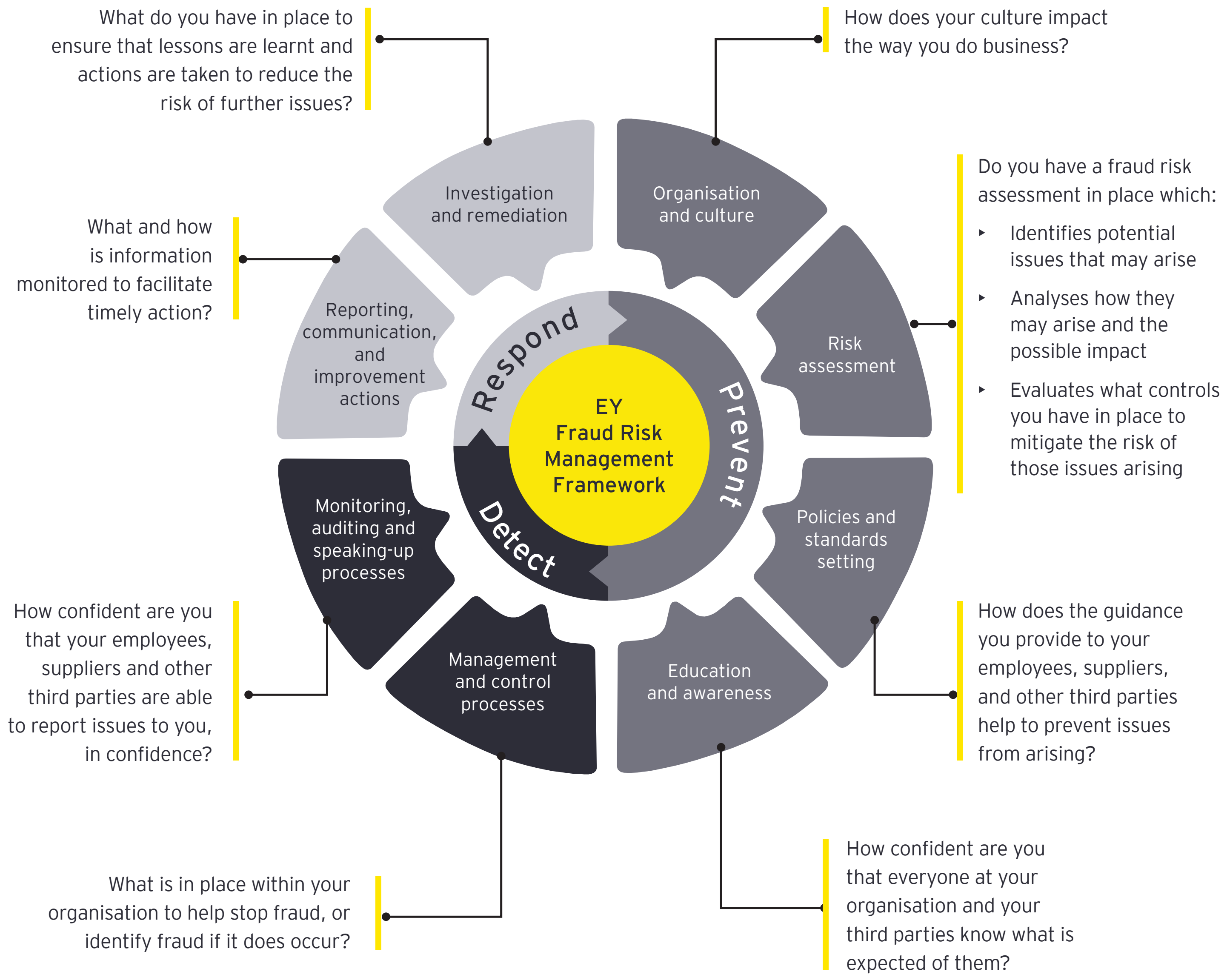
The legislation has been passed for Royal Assent and will be effective once the government has published its guidance on reasonable procedures which is expected by the end of 2024.

> "
>
> This is the most significant boost to the Serious Fraud Office's ability to investigate and prosecute serious economic crime in over 10 years.
>
> This new law will help prevent crime, as big businesses can no longer turn a blind eye to fraud. We also welcome the expansion of our search powers, which will help speed up our investigations.

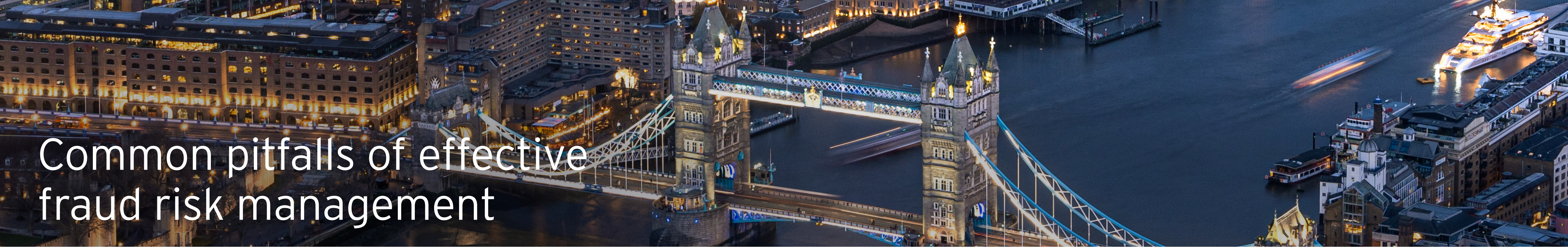
Nicholas Ephgrave QPM
Director of the Serious Fraud Office

How should your organisation respond to the new legislation?

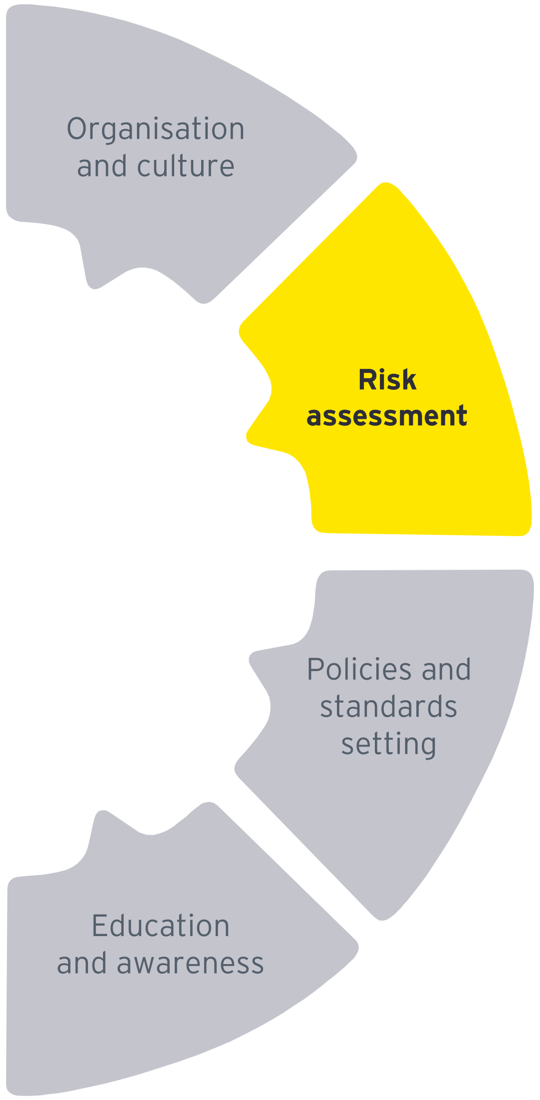
At EY, we have developed a comprehensive framework for effective fraud risk management, based on COSO principles and ACFE guidance, that has been implemented across many of our clients, in a variety of sectors. These eight core elements should form the foundation of your fraud risk management activities and integrate with your wider corporate governance and risk management structure.



Common pitfalls of effective fraud risk management



As fraud risk management is now becoming a business requirement for most organisations, it is important to acknowledge and appreciate the complexities of implementing and maintaining an effective programme. Doing so will foster strong stakeholder relationships and confidence while avoiding costly mistakes such as those illustrated below.



Fraud risk assessment

Overview

A holistic fraud risk assessment forms the foundation of your fraud risk management framework. It identifies and assesses fraud risk exposures to enable a risk-proportionate approach to fraud risk management. The prevent, detect and response elements of your anti-fraud framework should be informed and grounded by the results of the risk assessment.

Common pitfalls

Siloed approach

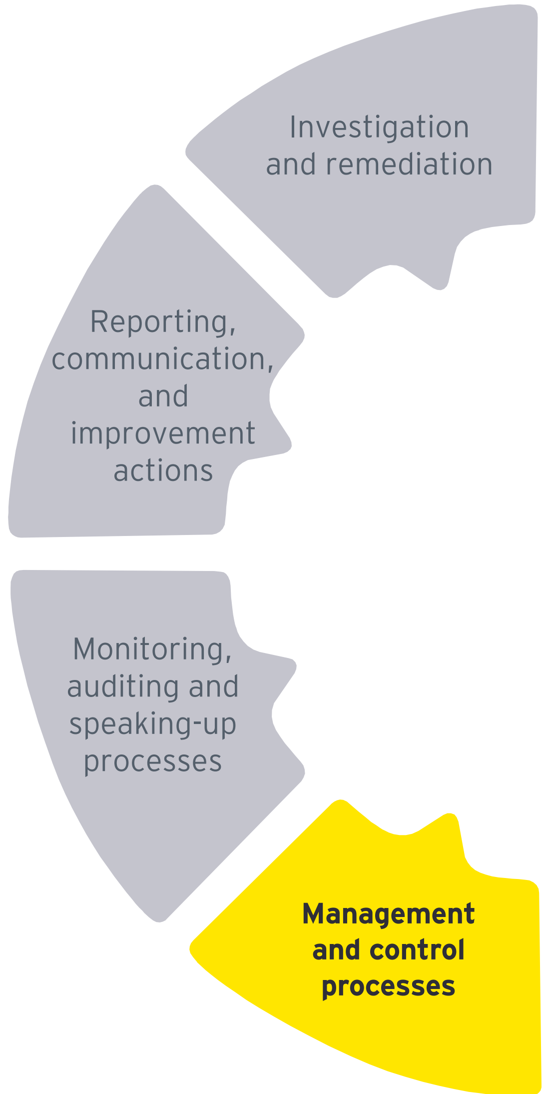
Some organisations conduct high-level, desktop-based fraud risk assessments that fail to appropriately consider all types of fraud and often result in generic risks that are difficult to apply to in day-to-day business activities and processes conducted by the business.

Reverse engineering

Some organisations work backwards from their existing internal controls to identify the potential fraud risks that they may address. This approach often limits the thinking to historic, traditional frauds rather than new and emerging frauds because of the changing internal and external landscape.

Control bias

Those involved in identifying and analysing fraud risks overlook or underestimate potential risk exposures as they assume 'that would never happen' due to already considering the controls that are in place. Control bias can lead to unidentified and/or incorrect prioritisation of fraud risks leading to mitigation efforts being misdirected.



Internal controls

Overview

Internal controls can work as deterrents and can help to prevent fraud when they are designed and operated with fraud risk in mind.

With growing scrutiny and potential corporate liability for failing to prevent fraud, internal controls over financial reporting (ICFR) and non-financial controls are essential for ensuring that financial reporting, procurement, operational, and commercial fraud risks are appropriately managed.

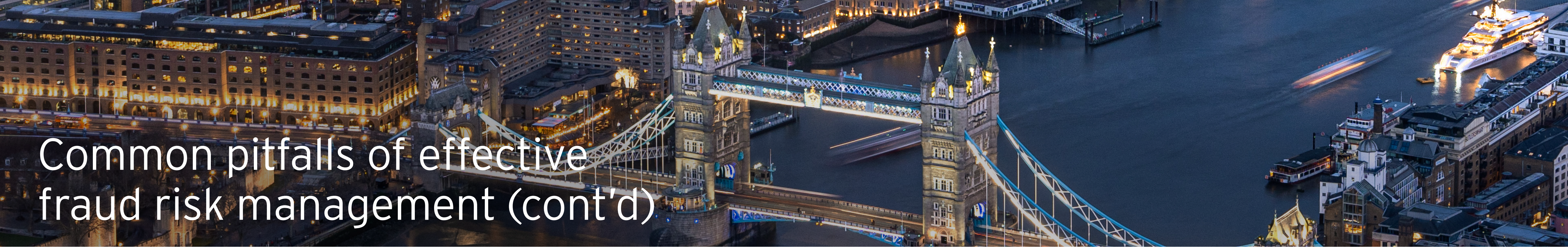
Common pitfalls

Tick-box mentality

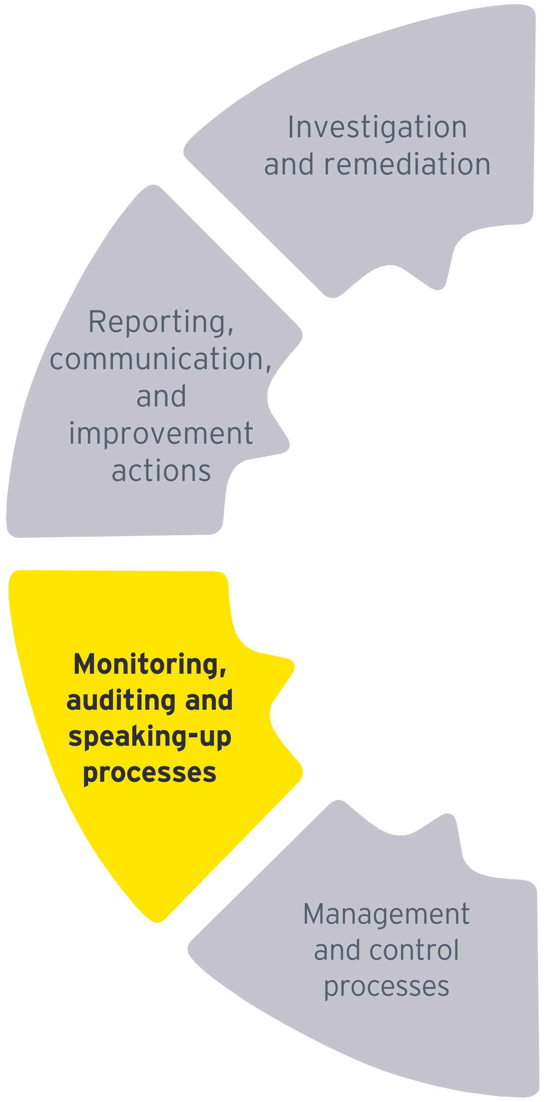
In our experience from fraud investigations, we know that control failures often arise due to a lack of understanding of control objectives by those operating them. For example, when an employee is signing off a bank reconciliation, they may see it as a 'tick-box' exercise – so long as the numbers balance everything is okay, and they can sign it off. They may fail to consider the need to review reconciling items to see if they look unusual or have been there for several months. This leaves the organisation exposed to fraud.

Lack of internal controls

Shockingly, for 29% of occupational fraud cases, the primary weakness identified was a lack of internal controls. From our experience, many organisations struggle to identify the key controls that mitigate their fraud risks. Failing to implement and articulate appropriate controls puts organisations at risk of fraud and destroys stakeholder confidence.



Common pitfalls of effective fraud risk management (cont'd)



Control evaluation and monitoring

Overview

Review and monitoring of internal controls is key to ensuring that they continue to protect your organisation. In addition, with 20% of occupational fraud involving the override of existing controls,[4] monitoring of activities and transactions in high-risk areas are also essential to identify trends and outliers that could indicate potential fraud.

Common pitfalls

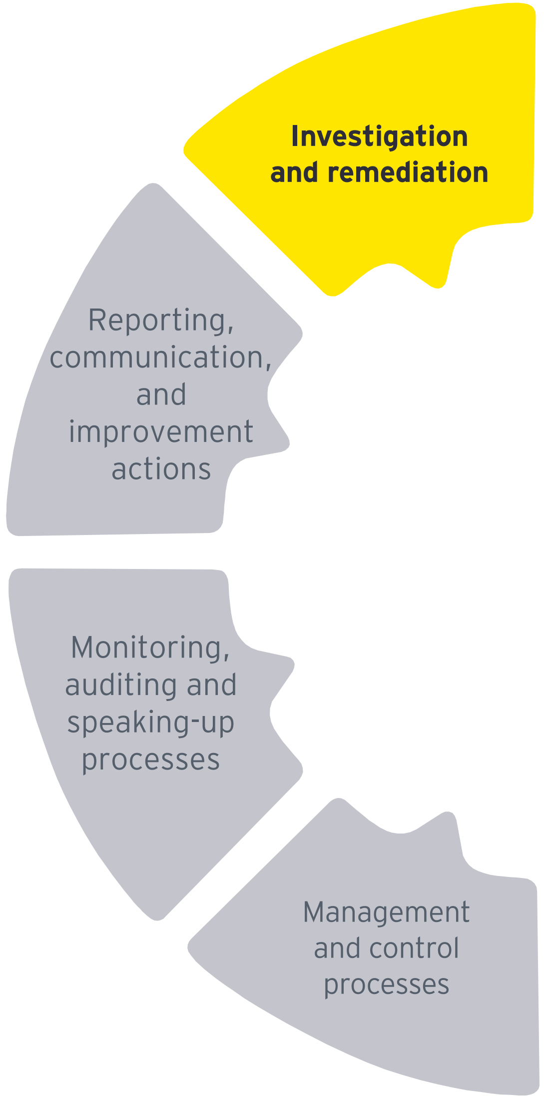
Set and forget mindset

Many organisations implement controls without considering the need to continually re-assess and evaluate those controls to ensure that they continue to be effective as the business and the operating environment evolve. As part of fraud risk management, evaluating and testing controls as part of a fraud risk assessment is key to validating those controls are effective in mitigating fraud risks. Often, ineffective controls are equal to no controls at all.

Overreliance on internal controls

It is commonly assumed that controls are sufficient in preventing fraud however, as one-fifth of frauds occur due to those controls being overridden, detective monitoring activities such as data-led screening of third-party payments for red flags have become an essential part of an organisation's defence against fraud. Despite this, most organisations fail to undertake any robust monitoring activities that could identify fraud red flags in a timelier manner.

4. ACFE: Report to the Nations (www.acfe.com)



Investigation and remediation

Overview

An organisation's response to potential fraud is critical to minimise losses and deter future instances of fraud.

Fraud surged by 24% during the COVID-19 pandemic.[5] At EY, we have seen an increase in fraud investigations since the pandemic and expect this trend to continue until well after economic pressures ease and new fraud schemes come to light.

Common pitfalls

Inadequate triage

Speak-up channels can be an effective way for organisations to identify wrongdoing such as fraud. However, many organisations have implemented speak-up channels without appropriate resources to conduct necessary triage activities. As triage is key to identifying and escalating potential fraud schemes for investigation, inadequate triage can result in frauds being missed entirely.

Strained resources

Despite more organisations having in-house investigation functions, many are under-resourced and lack the specialist knowledge and experience necessary to conduct investigations to the extent required. This ultimately results in potentially inappropriate conclusions and corresponding actions.

Groundhog Day syndrome

Once investigations are completed, most organisations mistakenly stop there and do not address the issues identified that resulted in the fraud occurring. Without identifying the root cause of issues and remediating any gaps and weaknesses identified, the organisation is likely to have similar frauds elsewhere in their business either now or in the future.

5. Victims Commissioner (www.victimscommissioner.org.uk)

Avoiding corporate criminal liability for failing to prevent fraud

Many organisations find themselves behind the curve and at risk of facing criminal prosecution. Those charged with governance, such as Audit Committee Chairs, are becoming increasingly concerned that their organisations may not have a robust and timely response to the new legislative landscape. With growing awareness and critical questions being asked by key stakeholders, including external auditors, organisations need to act now to keep up with the new requirements for fraud risk management.

Our clients have already partnered with us and leveraged EY's fraud risk management framework to address these concerns by understanding their current state, identifying any gaps and weaknesses, and co-developing a clear roadmap to implement and maintain a robust fraud risk management programme.

Many of our clients have found it useful to ask themselves these five questions to start to understand their challenges and seek advice from those experienced in developing and maintaining strong fraud risk management programmes.

Five key questions for those charged with governance

1. Is there a clear definition and consistent understanding of fraud across your organisation, and expectations of your employees and third parties to ensure issues are raised to you in confidence?

2. Who is accountable for managing fraud risk and are there clear responsibilities for individuals across your organisation?

3. Have you recently conducted a fraud risk assessment which:
    - Identified where you could be susceptible to fraud across your key business operations
    - Determines the level of your exposure in an objective and consistent manner
    - Enables you to effectively prioritise your resources in mitigating your fraud risks

4. What processes are in place within your organisation to detect instances of fraud and how is data used to enable timely detection?

5. Do you have the right people involved in investigating suspected fraud in your business and take steps to ensure that the fraud does not reoccur?

EY contacts

For more information on fraud risk management and to understand how your organisation needs to address these new requirements:

Emma Browne
Partner, Forensics

+ 44 7771 808 428
ebrowne@uk.ey.com

James Hensser
Director, Forensics

+ 44 7880 487 707
jhensser@uk.ey.com

Terry Seagreaves
Partner, Forensics

+ 44 7799 433 943
tseagreaves@uk.ey.com

Kar Wai Hau
Assistant Director, Forensics

+ 44 7552 271 053
khau1@uk.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EYSCORE 000967-24-UK

UKC-031137.indd (UK) 12/23. Artwork by Creative UK.
ED None

ey.com/uk