

Deloitte.

Fraud Risk

Building confidence in your fraud risk framework



Contents



1

Introduction



2

Expectations on fraud risk management



3

Key themes behind recent fraud cases



4

Creation of a robust fraud
risk management framework



5

Key steps to enhance fraud risk management



6

Conclusions



7

Contacts



1. Introduction



High profile fraud is becoming more common place leading to many organisations suffering both financially and reputationally. With the pandemic driving a widescale move to remote working there has been a surge in fraud and scams, ranging from identity theft and cyber fraud, to manipulation of COVID-19 government support schemes.¹ Recent research has estimated losses from fraud to be in the region of £140bn per year.²

The Royal United Services Institute (RUSI), the world's oldest defence and security think tank, notes "*Fraud has reached epidemic levels in the UK and should be seen as a national security issue*".³

Against this backdrop there is increased focus and desire to strengthen the responsibility and accountability of those charged with governance on the prevention and detection of fraud from the government and regulators.

Organisations are increasingly considering how they **improve** their fraud risk assessment and fraud risk management frameworks to help protect against future financial loss and reputational damage.

This paper will examine the drivers for the increased appetite for effective fraud risk management and how to create increased levels of confidence over fraud risk frameworks, exploring the following areas:



Expectations for management and those charged with governance on fraud risk management



Key themes behind recent fraud cases



Creation of a robust fraud risk management framework



Increasing confidence over fraud risk management

1. <https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf>

2. <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime>

3. <https://www.bbc.co.uk/news/business-55769991>



2. Expectations on fraud risk management



In the current economic climate, organisations may be more prone to fraud risk both internally and externally. This may be a result of a desire to “improve” financial results in the aftermath of the COVID-19 pandemic or due to the increasing levels of sophistication of fraudsters and their scamming techniques.

Despite the high number of fraud cases, the increased focus on fraud by stakeholders and the broader societal expectations for more transparency in respect of fraud risks and mitigating controls, many organisations still do not have formal or adequate fraud risk management frameworks and are exposed to significant losses and regulatory scrutiny if they do not take action.

However, the responsibilities of those charged with governance and management in relation to prevention and detection of fraud has not changed.

For example, the FCA expect (i) “... senior management to take clear responsibility for managing financial crime risks, which should be treated in the same manner as other risks faced by the business” and (ii) “... a firm to consider the full implications of the breadth of fraud risks it faces, which may have wider effects on its reputation, its customers and the markets in which it operates⁴”.

The FCA’s regulatory requirement is also supported in other guidance such as the COSO Fraud Risk Management Guide⁵.

“Senior management has overall responsibility for the design and implementation of a Fraud Risk Management Program, including setting the tone at the top that creates the culture for the entire organization. The board establishes policies and procedures explaining how the board provides oversight, including defining expectations about integrity and ethical values, transparency, and accountability for the implementation and operation of the Fraud Risk Management Program.”

The role of management reporting has also been highlighted. For example, in the Brydon report⁶ which notes the following:

“It is clear that ‘the extent to which fraud can be detected is dependent on the quality and timeliness of management reporting, and the openness of the corporate culture’, and the first part of the Standard on Fraud stresses that management and the Board are responsible for preventing and detecting fraud.”

The above statements are also echoed by the White Paper published in March 2021: “Restoring trust in audit and corporate governance”⁷ where the role of financial reporting is also examined.

Building on the potential changes coming out of the BEIS White Paper, in June 2021, the Law Commission launched a consultation regarding whether, and how, the law relating to corporate criminal liability can be improved so that it appropriately captures and punishes criminal offences committed by corporations, and their directors or senior management. One potential outcome of this might be an extension to current 'failure to prevent' offences that exist for bribery and tax evasion under the Bribery Act 2010 and Criminal Finances Act 2017 respectively ⁸.



4. <https://www.handbook.fca.org.uk/handbook/FCG.pdf>

5. <https://www.coso.org/Documents/COSO-Fraud-Risk-Management-Guide-Executive-Summary.pdf>

6. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/852960/brydon-review-final-report.pdf

7. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/970676/restoring-trust-in-audit-and-corporate-governance-command-paper.pdf

8. <https://www.lawcom.gov.uk/law-commission-see-views-on-corporate-criminal-liability/>

3. Key themes behind recent fraud cases



The risk of fraud is driven by a diverse set of factors. This includes the risks inherent in the business model, the complexities of judgements in accounting, the employee mindset (incentives) and the exposure of business data to internal and external attacks.

The culture of the organisation, and particularly the tone from the top, is also a critical factor underpinning the fraud risk environment, as is the reinforcement of the values through middle management and the robust nature of the internal control environment.

In the diagram we present some key thematic root causes of fraud based on a range of recent cases with several examples of how they may manifest.

EXAMPLES



Cyber risk

- Spam / phishing emails not blocked / poor user practices and insufficient restrictions
- Lack of cyber security training
- Weak system access controls



Inherent business risk

- Fraud risk created due to the nature and location of (i) business operations (e.g. remote / hybrid working) and (ii) oversight / controls
- Recent change in performance or stretching business strategy



Covid-19

- Fraudulent applications for the government schemes for example Bounce Back Loans or furlough schemes



Tone and overall culture

- Inconsistent tone from the top and middle. Culture where fraud is not taken seriously (e.g. incidents are not reported or acted upon). Dominant personality at the top
- Related parties and close relationships that are not appropriately considered for fraud
- Misleading auditors and advisors to conceal fraud through false statements and window-dressing
- Incremental pressure on reported numbers / management control override



Accounting treatment risk

- Management judgments and positions not challenged
- Revenue and expense recognition of long term contracts not being properly accounted for and hence inflating performance



Control environment design and effectiveness

- Control environment reliant on aged, unintegrated systems, with manual controls / workarounds and a history of control weaknesses
- Bank reconciliations not performed appropriately and reconciling items not investigated properly
- Expense claims not adequately reviewed to identify theft
- Physical verification of assets not performed adequately

1



2



3



4



5



6



7



4. Creation of a robust fraud risk management framework



As is evident in the themes highlighted on page 5, fraud risk can arise in a variety of different ways requiring robust fraud risk management to protect organisations. With this evolving fraud risk landscape in mind, organisations should ensure they have a fraud risk framework that:

- a) **is integrated into the overall risk management framework;**
- b) **is embedded and visible within all areas of the organisation;**
- c) **develops a culture which supports the prevention, detection and deterrence of fraudulent behaviour;**
- d) **is regularly assessed, with controls redesigned where vulnerability to fraud is identified; and**
- e) **responds to address fraud swiftly.**

The above is important for senior management and directors to protect and sustain the business, discharge their duties, be alert to where risks reside and intervene with strong controls, and respond to regulatory reform as and when it is required.

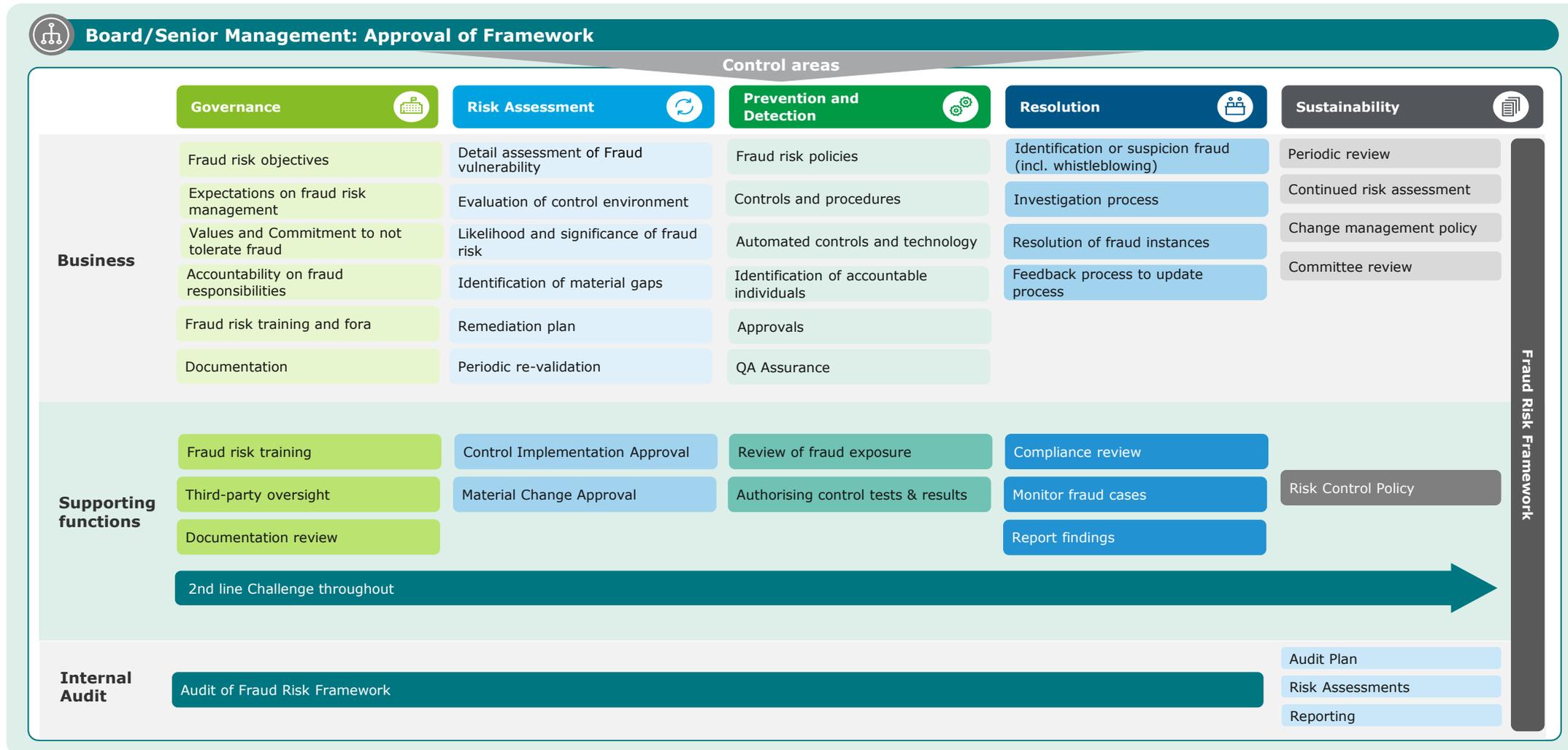
Based on our experience, an effective framework should contain a number of different components. This is illustrated in the diagram below. Organisations should continually consider how their current framework is designed and operating in practice in light of a heightened and dynamic fraud risk environment.



4. Creation of a robust fraud risk management framework



Fraud Risk Framework



5. Key steps to enhance fraud risk management

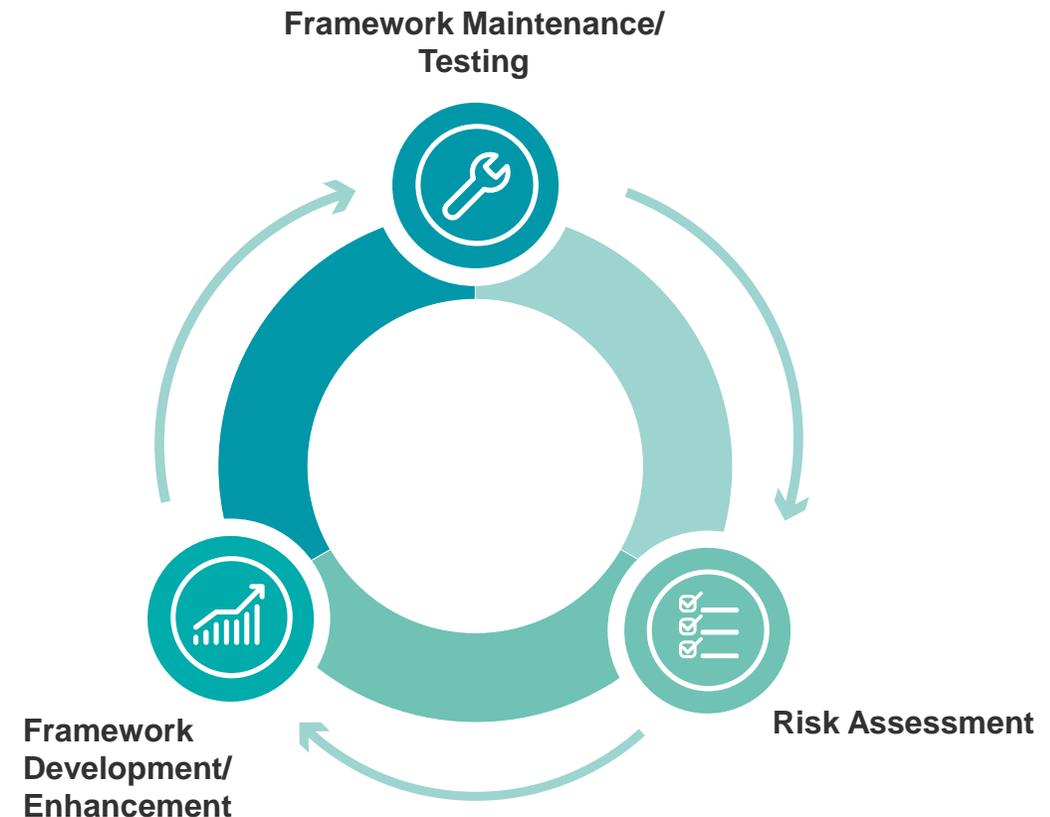


As highlighted previously, the government and regulators are increasing their focus on fraud risk management. The current environment makes it an even greater priority for organisations to gain comfort over their fraud risk frameworks, in areas such as:

- fraud risk assessment;
- design and operating effectiveness of the fraud risk management framework;
- processes and controls operated by 3rd parties; and
- documentation of the end to end process.

Increasing confidence levels in these areas will better enable senior management to discharge their duties and be ready to respond to increased regulatory and stakeholder scrutiny in relation to fraud risk management. Further, there are additional benefits in terms of supporting sustainable business practices which should not be overlooked.

In the remainder of this paper we explore key steps to increase levels of confidence over an organisation's fraud risk management framework. Whilst we do not discuss the different approaches which organisations may ultimately use to gain assurance over their fraud risk management framework, we note three fundamental focus areas which organisations may consider when seeking to enhance confidence over the fraud risk framework; namely, (i) risk assessment refresh, (ii) framework development / enhancement and (iii) framework maintenance / testing. These will be examined in the following sections.



5. Key steps to enhance fraud risk management (cont.)



Refresh the fraud risk assessment

Organisations should evaluate their existing fraud risk frameworks to understand whether their fraud risk assessment and governance is sufficient to prevent and detect material fraud considering areas such as fraud risk in financial reporting, misappropriation of assets, operational fraud risks, etc. The fraud risk assessment process is a fundamental building block of fraud risk mitigation. Amongst other considerations, the following areas are examples of focus areas when analysing the adequacy of the current fraud risk assessment:

Business environment (current and future) – Assess whether the environment exposes the organisation to new fraud risks or increases the threat of existing fraud risks.

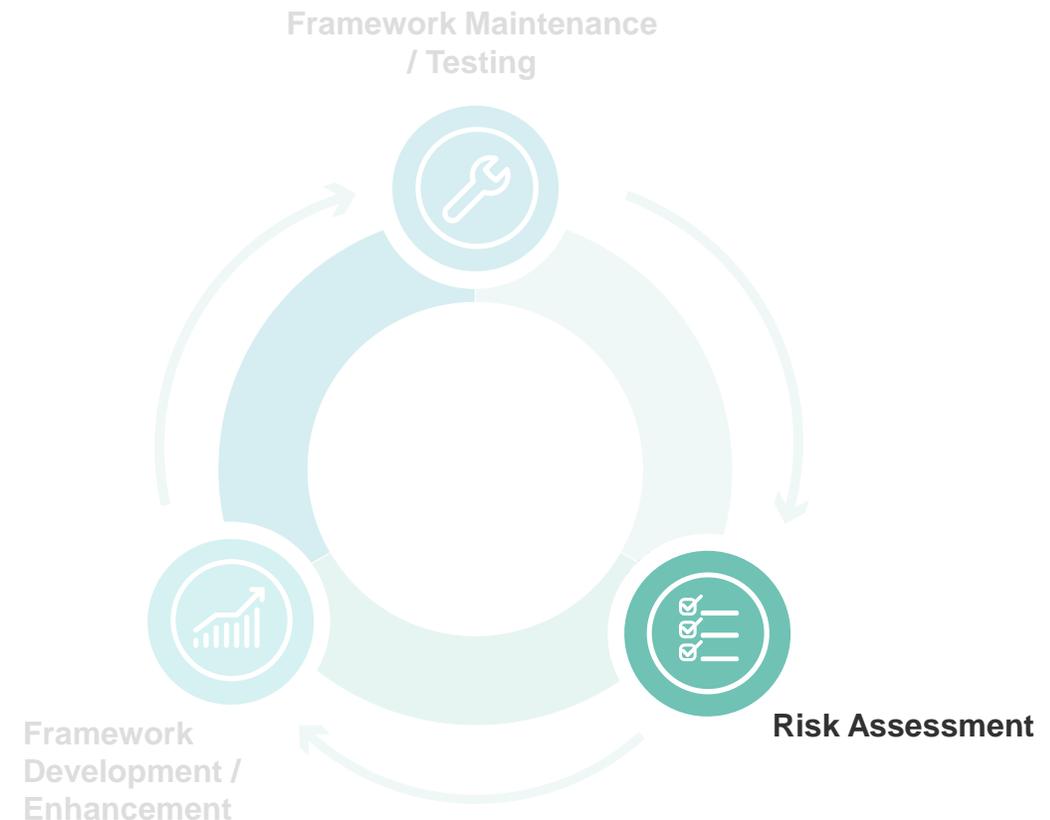
Business operations and locations (existing and new) – Consider whether the fraud risk assessment is consistently applied across all business areas and locations.

External parties – Whilst internal threats remain, review the risks that 3rd party firms and organisations bring and consider the extent to which some are heightened by the current environment and business activity.

Reporting – Understand the reporting that senior management receives on the fraud risk assessment to enable informed decision making and to facilitate their oversight and challenge of the fraud risk assessment process itself.

Documentation – Consider whether the fraud risk assessment is demonstrable and evidences judgements and conclusions clearly. This will facilitate a robust analysis and review of fraud risk, and evidence how the firm has considered the impact of fraud risk on its business and operations.

This exercise is a key step on the pathway to building comfort over the adequacy of the framework and will allow organisations to identify (i) vulnerability to fraud, (ii) significant gaps in the control environment and (iii) suspicion of real fraud instances.



5. Key steps to enhance fraud risk management (cont.)



Review the control framework

A renewed focus on the fraud risk assessment will facilitate a refreshed analysis of the adequacy of the control framework to mitigate heightened areas of fraud risk. This phase is critical as it reinforces the foundations of an appropriate fraud risk framework. The steps outlined below will help organisations respond to gaps and enhance the framework's effectiveness. Organisations should involve different business areas and control functions when considering the following:

Prioritisation – Identify which control gaps require immediate attention or expose the organisation to higher fraud risk.

Technology – Understand whether any smart technology, artificial intelligence or other intelligent tools can be deployed to support fraud detection and prevention.

Plan – Evaluate how long is required to address the gaps, implement new technologies and complete fraud-related investigations.

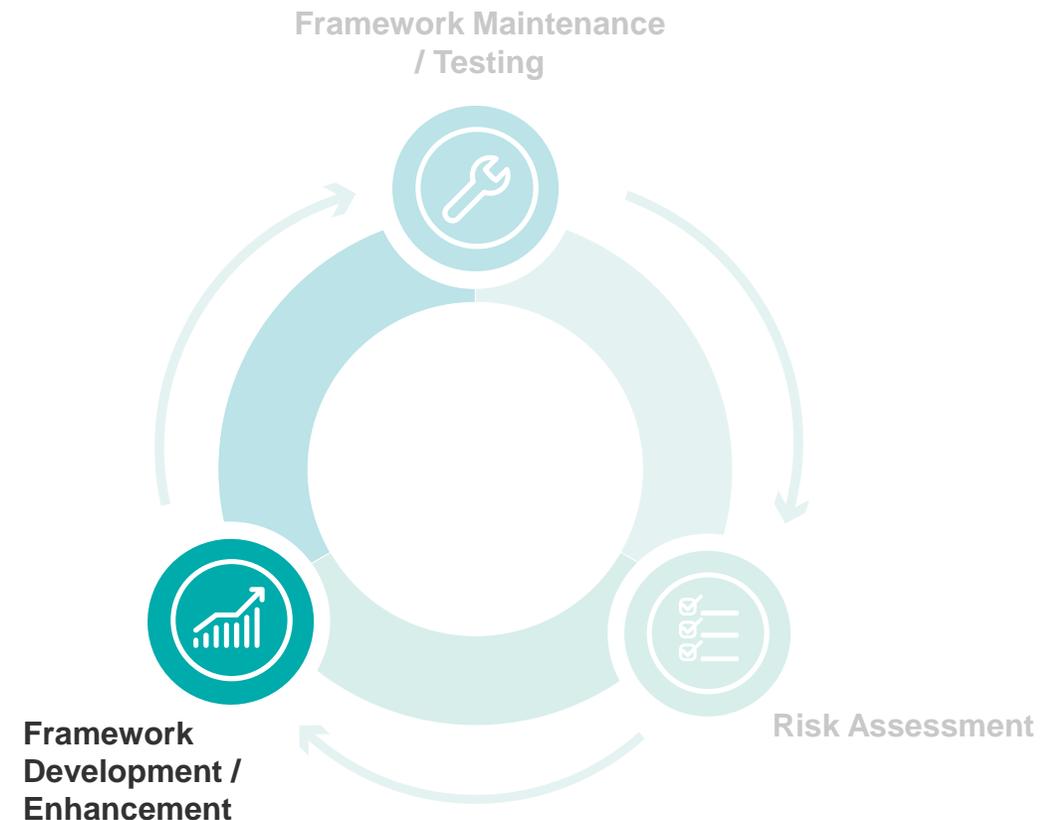
Use of specialists – Consider the need for a dedicated team specialising in fraud risk management or external support (where relevant).

Communicate / train – Assess how changes will be communicated and what training is needed to ensure all staff are committed to fraud deterrence.

Evidence – Documentation of all existing and new procedures, process and controls including an assessment of any new technological solutions relied on to prevent and detect fraud.

Sustain – Assess the methods that should be used to embed the enhanced framework into the heart of the business and maintain it going forward

It is crucial that the control framework is consistently and accurately documented across the organisation, including a clear view of fraud risks and the preventative and detective controls in place. The maintenance of such a documentation set better facilitates management's ability to articulate its framework both internally and externally.



- 1 →
- 2 →
- 3 →
- 4 →
- 5 →
- 6 →
- 7 →

5. Key steps to enhance fraud risk management (cont.)



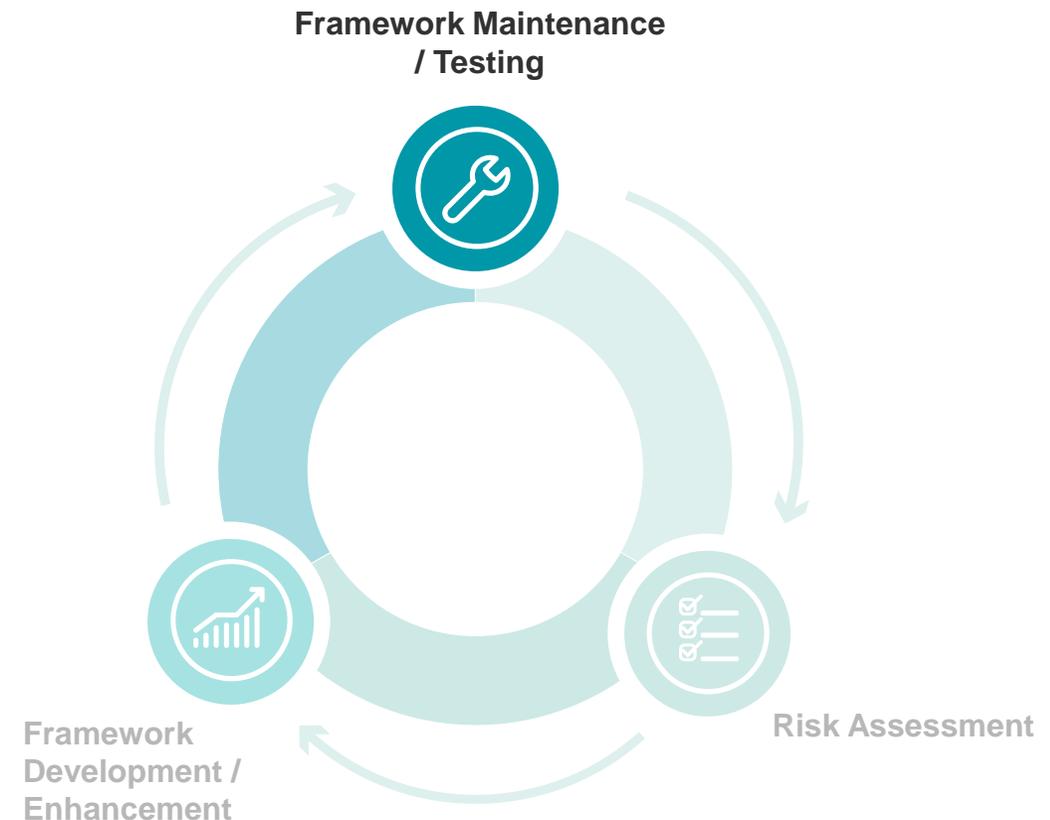
Maintain and test the framework

Fraudsters' tactics continually change; they become more sophisticated and find new methods to commit fraud. Therefore, organisations should not become complacent after they have made the necessary improvements to their fraud risk framework. As fraudsters' methods evolve, businesses should frequently assess where they have vulnerabilities and address them, using internal control functions and external specialist teams to continuously monitor performance of the framework and identify gaps or ineffective processes.

Organisations, amongst others, should consider the following in their testing phase:

- a plan to incorporate evaluations which are both ongoing and specific to areas of concerns;
- the degree of business / operation changes;
- use of employees with relevant experience to undertake the reviews; and
- assessing the testing's performance and whether it requires amendment.

As touched on above, the formalised process which an organisation can point to in order to demonstrate the sustainability of its fraud risk management framework in light of evolving risks and changing business activities is the final key step in building confidence and likely of interest to any stakeholder seeking to challenge the adequacy of the framework. Finally, it will also help align with the growing expectations around financial reporting controls.



6. Conclusions



It is clear that fraud is not an issue that will simply 'go away'. Further, with new legislation and more intense public and regulatory scrutiny it is essential for management to act now to ensure that:

- fraud risk is appropriately identified
- exposure to fraud risk is appropriately mitigated;
- their organisation is able to demonstrate how its fraud risk management framework operates;
- the organisation is ready to comply with future UK SOX requirements (a 12-18 month journey); and
- the required duties of stewardship are properly discharged.

Our Fraud Risk practice is comprised of professionals with deep forensic, fraud advisory and assurance expertise. We specialise in supporting organisations go through this journey to prepare and gain confidence over their fraud risk management framework and fraud risk assessment.



7. Key contacts



If you would like to discuss any matters related to Fraud Risk or have any questions, please contact:



Mark Cankett
Partner, Global Fraud
Assurance Lead
mcankett@deloitte.co.uk
+44 20 7007 5150



Jules Colborne-Baber
Partner, Forensic Fraud Lead
jcolbornebabber@deloitte.co.uk
+44 20 7303 2905



Sonya Butters
Partner, UK Sox Lead
sobutters@deloitte.co.uk
44 7789 874877



Simon Cuerden
Partner, Fraud Forensic
scuerden@deloitte.co.uk
44 20 7007 2020



James Meadowcroft
Director, Risk Advisory Fraud
Lead
jmeadowcroft@deloitte.co.uk
44 161 455 6715



Ian Hughes
Director, Forensic Fraud
iphughes@deloitte.co.uk
+44 161 455 8831



Rob Wylie
Director, Forensic Fraud
Specialist
rwylie@deloitte.co.uk
+44 20 7303 2535



Fraser Beveridge
Director, Global Fraud
Assurance
frbeveridge@deloitte.co.uk
+44 20 7303 5851



Christos Doulas
Associate Director, Global
Fraud Assurance
chdoulas@deloitte.co.uk
+44 20 7303 6961





Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte’s more than 200,000 professionals are committed to becoming the standard of excellence.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2021. For information, contact Deloitte Touche Tohmatsu Limited.