A&O SHEARMAN

Reasonable procedures to prevent fraud: practical tips for large organisations

26 November 2024

We distil key practical takeaways from the UK Government's official guidance on the corporate criminal offence of failure to prevent fraud (the **Guidance**).

Businesses and compliance teams will be working to review and prepare fraud prevention procedures for the September 1, 2025 implementation date. A complete defence to the new failure to prevent fraud offence is available where an organisation can show it had reasonable fraud prevention procedures in place, or it was not reasonable to expect it to have such procedures.

New detailed guidance on 'reasonable procedures'

The Guidance offers detailed information to help businesses align their preparation efforts with the inherent fraud risks in their operations. It acknowledges that an organisation's fraud prevention plan should be proportionate to its risk and potential impact, recognising that different risks will exist for different organisations. Many businesses already have policies in place to prevent fraud on the business, but not necessarily for fraud by the business or those providing services on its behalf.

The Guidance is not prescriptive but rather flexible. A deviation from it does not automatically imply that an organisation lacks reasonable fraud prevention procedures. The Guidance is a useful starting point for organisations in the early stages of designing and implementing their fraud prevention strategies. By adhering to it, businesses can better mitigate the risk of fraud being committed by an associated person, as well as the risk of criminal prosecution.

The Guidance has a particular focus on six familiar principles:

1. Top level commitment

The board of directors, partners and senior management are expected to "foster a culture within the organisation in which fraud is never acceptable" and "should reject profit based on, or assisted by, fraud." Best practice is suggested to include:

- A list of "designated responsibilities" for fraud prevention among senior management, including horizon scanning, development of disciplinary measures (with the consequences

for committing fraud articulated), whistleblowing and investigation of fraud which is detected or suspected.
- Adequate access for the Head of Compliance (or a similar role) to the board or CEO (even if they have another direct reporting line).
- Budget specifically committed for the fraud prevention plan (whether leadership and training, third party due diligence (DD) or DD related tools), including long term resourcing and sustaining of anti-fraud practices when key members of staff are off work.
- Leading by example with an open culture, where staff are encouraged to speak up early if there are any ethical concerns.

The Guidance suggests that, for organisations subject to the FCA's Senior Managers and Certification Regime, the lead senior manager for the purposes of failure to prevent fraud may be the same person as the Senior Manager with responsibility for an organisation's financial crime compliance systems and controls; or if not, that they should work closely with that individual.

2. Risk assessment

There is significant and pragmatic emphasis on risk assessment, which is crucial given the variety of base fraud offences covered by the failure to prevent fraud offence. Organisations should, assisted by sources of information such as data analytics, previous audits, sector specific information and regulator enforcement actions in their sector:

- Recognise that the definition of an associated person is wide and identify different typologies of associated person such as agents, contractors or staff in sensitive roles or departments.
- Consider the circumstances in which each category of associated person could assist or commit one of the fraud offences.
- Develop a typology of risk looking at the 'fraud triangle' to understand the organisation's inherent fraud risk:

1. Opportunity: where do opportunities to commit fraud that benefits the business or customers exist? Which departments or roles have the greatest risk exposure, either due to their subject matter or structure (for example, by lack of independent oversight)?
2. Motivation: look at the structure of the reward and recognition system. Are there financial and operating pressures on staff which may incentivise fraud?
3. Rationalisation: consider the organisation's culture, and whether it is 'quietly tolerant' of fraud. Also look at whether fraud is prevalent in the organisation's particular business sector.

3. Proportionate risk-based prevention procedures

The business should draw up a "fraud prevention plan" proportionate to the fraud risks it faces (as identified in its risk assessment), and the nature, scale and complexity of its activities.

The Guidance recognises that the level of prevention procedures considered to be reasonable should take account of the level of control and supervision the organisation is able to have over a

particular person acting on its behalf and the relevant body's proximity to that person. So the procedures will allow for greater control over the conduct of an employee vs an outsourced worker performing services on its behalf (where appropriate controls should be implemented via relevant contractual terms, as we have seen in practice with anti-bribery measures).

The prevention procedures should reduce the opportunity and the motive for associated persons to commit fraud, such as through:

- Pre-employment and vetting checks.
- Regular anti-fraud training, that is evaluated and monitored appropriately.
- Amending bonus frameworks that encourage risk-taking, or working to prevent time-pressured working conditions that encourage staff to cut corners, to ensure that fraud is not encouraged.
- Collecting information on potential conflicts of interest and keeping such information under review.
- Examining internal disciplinary and reporting procedures, with consideration given to reporting outcomes of fraud-related investigations, not only to staff but other associated persons.
- Reducing rationalisation of fraud by stressing that fraud is the responsibility of everyone in the organisation, and incorporating a reminder into performance evaluations.

Any decision not to implement procedures in response to a specific risk (which, according to the Guidance, may be deemed reasonable in "some limited circumstances") should be documented "together with the name and position of the person who authorised that decision" and reviewed at appropriate intervals.

Best practice involves regular stress testing the effectiveness of the fraud prevention procedures by members of the organisation not involved in writing it. Regular stress testing is an obligation which will be familiar to some large corporates under the UK Corporate Governance Code, but the Guidance also cautions that simply stating that the business is compliant with the Code, or other regulatory requirements, would not be a suitable defence.

4. Due diligence

Organisations are expected to apply due diligence to persons who perform or will perform services for or on behalf of the organisation, or when acquiring a third party in any merger or acquisition. Such processes will be familiar to many organisations and best practice is described as including the use of appropriate technology such as risk management tools, screening tools, vetting checks etc. The inclusion of fraud should be an extension, clearly articulated in the due diligence procedures, rather than wholesale replacement of existing processes. Contracts with associated persons should be reviewed for appropriate obligations requiring compliance and ability to terminate in the event of a breach.

The Guidance sets out best practice for M&A, and notes that where businesses being acquired are not 'large organisations' they may not have measures in place that directly address the offence, and therefore a key consideration will be the integration of fraud prevention measures post-acquisition.

Interestingly, the Guidance also suggests monitoring of staff and agent wellbeing as best practice, recognising that people may be more likely to commit fraud due to stress, targets or workload

5. Communication (with the expectation of proactive training)

Organisations are expected to embed an internal understanding of fraud prevention policies and procedures through training, in a way that is proportionate to the fraud risk that each group (staff or contractors) faces as identified by the company's risk assessment. They must also consider integrating anti-fraud messages into existing policies such as those related to sales targets or customer interactions.

The expectation that fraud prevention is the responsibility of all within the organisation is repeated here; communication "should be from all levels within an organisation", acknowledging the dangers of middle management undermining messages from senior management.

Training must ensure that staff and other associated persons are familiar with whistleblowing policies, and that managers know how to respond when whistleblowing concerns are raised. Businesses may also feel that it is necessary, to ensure that there is an awareness and understanding of policies by associated persons who are not employees, to require certain representatives to undertake fraud-specific training too. The Guidance notes that they may choose to train third party associated persons or encourage them to ensure their own arrangements are in place.

The Guidance is particularly detailed on training to challenge fraud rationalisation, eg by encouraging proactive challenges to thinking that can lead to fraud being rationalised by wrongdoers. Training must be kept under review, and effectiveness of training should be monitored over time.

A section dedicated to whistleblowing includes board level accountability to oversee whistleblowing, ensuring that reporting channels for whistleblowers are independent and training staff to ensure they know how to respond to whistleblowing concerns when raised.

6. Monitoring and review

Fraud prevention is not a 'one and done' process. Organisations are expected to periodically re-examine the performance of their fraud prevention frameworks, learn lessons from detected or attempted fraud (including from investigation and whistleblowing incidents and reviewing information in its own sector) with escalation of management to board level.

Monitoring is broken down into three elements: (1) detection of fraud and attempted fraud; (2) investigations (noting that these should be 'independent', 'appropriately resourced, empowered and scoped' and 'legally compliant' and (3) monitoring effectiveness of fraud prevention measures. Considerations for organisations relating to these first two elements are set out in a series of questions which organisations are encouraged to ask, such as:

1. For detection: What analysis is carried out? Through what tools? Is there scope for AI? Are staff encouraged to speak up? Is there a nominated member of staff to collate and verify the management information (MI) on suspected fraud for flagging to the board?
2. For investigations: What factors would trigger an investigation? Who authorises them? Are decisions to investigate documented? What factors determine whether the investigation is internal or external? What measures are in place to ensure investigations of potential fraud are independent? What arrangements are there for the results of investigations to be reported on to the board? How are outcomes and lessons learned disseminated within the organisation where appropriate?

Monitoring includes data on training, updates to procedures including DD, financial controls and updates to contractual clauses for associated persons.

Reviews are expected to recognise that fraud risks will change and evolve over time and therefore the fraud procedures need to be adaptable. Organisations may wish to have their reviews conducted either by external parties or internally, but either way, should seek internal feedback, examine the outcomes of investigations and whistle-blowing cases and subsequent actions taken, examine relevant findings such as prosecutions and deferred prosecution agreements and collate and verify MI on the effectiveness of the fraud prevention measures and flag these to the board.

What organisations can do now

Businesses within the scope of the new offence may have already begun preparations, as the government initially indicated a six-month implementation period, which has now been extended to nine months (and in fact is more like ten months).

For those just starting out on their journey, the initial focus should be on ensuring a top-level commitment to fraud prevention, as advised in the Guidance. This includes setting agreed milestones, establishing budget and resourcing, and agreeing a clear timeline to achieve full implementation by no later than September 1, 2025. After that point, businesses face the risk for conduct after September 1 not only of investigation by government enforcement agencies including (as flagged in the Guidance) by the Pensions Regulator, or the Financial Conduct Authority under their specific prosecution powers in relation to fraud, but also private prosecutions.

The first critical step is to conduct a comprehensive risk assessment for the organisation, including identifying which parts of the organisation may be in scope (extra-territorially) for the offence. The Guidance emphasises that this is a foundational step towards establishing reasonable fraud

prevention procedures, noting that "it will rarely be considered reasonable not to have even conducted a risk assessment". This may involve revising or extending existing risk assessments rather than starting from scratch. A thorough understanding of the underlying fraud offences covered by the new legislation, including the territorial scope of each, and the entities and individuals likely to be considered 'associated persons' are essential.

Following the conduct of the risk assessment, organisations will need to develop a reasonable and proportionate “Fraud Prevention Plan” tailored to their specific risks; this is almost certain to include the need to conduct an overarching review of existing policies and procedures (in particular whistleblowing), and to implement a review or development of anti-fraud training provided to staff and other ‘associated persons’. We also expect that many organisations will want to consider and introduce anti-fraud contractual protections (as many organisations did following the introduction of s7 Bribery Act).

Internal teams should consider reviewing and revising their play books for investigations (if they have one, and introducing one if not), ensuring that where any potential fraud is suspected or reported, the organisation has a mechanism for considering whether it is in scope of this offence, and that its investigation and internal reporting procedures for in-scope suspected fraud are followed.

Finally, once the fraud prevention framework is in place, the organisation will need to develop a plan for ongoing monitoring and review. This includes learning from and acting to enhance procedures based on internal incidents, any issues flagged in audits, reviewing information from the business sector, as well as incorporating any relevant legal developments affecting the scope of the underlying fraud offences.

A congested ecosystem of other fraud related rules and codes of conduct

Many businesses have expressed concerns about the potential overlap between the new failure to prevent fraud offence and existing regulations and corporate codes of conduct. The Guidance explicitly acknowledges this. Whilst duplication of effort is not expected, businesses cannot assume that their existing policies and procedures will fully address the requirements of the new offence, even if they are already regulated by bodies such as the Financial Conduct Authority. Instead, businesses must consider the specific external fraud risks posed by different categories of associated persons and implement appropriate fraud prevention policies tailored to the new offence.

Our fraud and corporate specialists can help advise on all or any aspects of the new offence, preparation for implementation, and how to respond.

Our earlier blog post explored what the UK Government’s recently published guidance on the failure to prevent fraud offence reveals about how the new offence may be used (the Guidance)