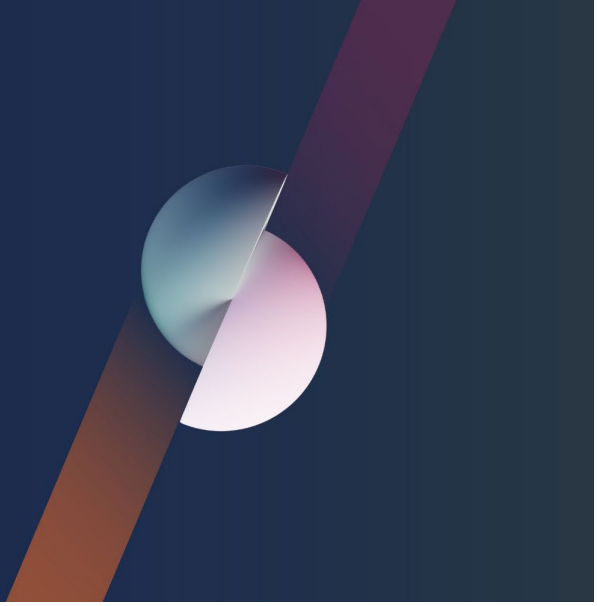
SLAUGHTER AND MAY/

20 NOVEMBER 2024

COUNTDOWN TO COMPLIANCE – FAILURE TO PREVENT FRAUD GUIDANCE RELEASED



The UK government has released its long-awaited Guidance on the new corporate offence of failure to prevent fraud, outlining the key elements of the offence and offering practical advice on designing and implementing reasonable fraud prevention procedures. The new offence will come into force on 1 September 2025, giving organisations a significant implementation period of nearly 10 months.

How significant is this?

The Government has stated that it envisions the new offence will drive a significant shift in corporate culture around fraud prevention, akin to the changes prompted by the introduction of the failure to prevent bribery offence in the UK Bribery Act 2010 (UKBA). However, the response by companies to the new offence has, in our view, been calmer than was the case in 2010, likely because the compliance culture and processes of many (although not all) organisations has significantly matured over the past decade and more. Today, organisations are well-versed in possible corporate criminal liability for 'failure to prevent' offences, and compliance practices have become increasingly sophisticated.

The Serious Fraud Office (SFO) has endorsed the new offence, with Director Nick Ephgrave urging organisations to "get their houses in order" to avoid potential criminal investigation. However, this aggressive language may be somewhat overstated. The new offence does not stem from a sudden surge in fraud committed by corporates, many of which already have strong compliance frameworks in place. For many, the new Guidance will build upon their existing compliance ecosystem, rather than requiring an overhaul.

Nevertheless, even organisations with strong compliance frameworks will need to make significant preparations before the offence takes effect. The new offence is undoubtedly broad, as a wide range of misconduct by employees and others, could be captured under the definition of 'fraud' used in the legislation. Implementing procedures to prevent these behaviours will require more nuanced changes than those needed for more easily identifiable offences like bribery, tax evasion or cartel activities. The lengthy implementation period is an acknowledgment that organisations will need to, at least, undertake a process to assess whether their existing processes align with the expectations set out in the new Guidance, in light of the fraud risk profile of their particular business.

Recap on the offence

The new offence will mean that large organisations[1] may be criminally liable if someone associated with them (such as an employee, agent, subsidiary, or someone performing services for or on their behalf) commits fraud with the intention of benefitting the organisation (or any person who receives services from the organisation, eg. a client). It does not need to be shown that the executives or senior managers knew about or even suspected the fraud. Importantly, an organisation will have a complete defence if it can prove (on a balance of probabilities) that it had 'reasonable' procedures in place to prevent fraud at the relevant time. The concept of such a defence should be familiar from existing 'failure to prevent' offences.

[1] Meaning an organisation which meets two of the following three criteria: a turnover of more than £36 million, more than £18 million in total assets, or more than 250 employees. These criteria apply to the whole organisation, including subsidiaries.

The new offence only applies if the base fraud has some connection to the UK, meaning that at least one aspect of the base fraud must occur in the UK, or the gain or loss from the fraud must have occurred or been intended to occur in the UK. The offence will not apply to fraud committed abroad, provided there is no UK nexus. This contrasts with the failure to prevent bribery offence, which can bite on organisations that have a business in the UK even when all elements of the base offence occur overseas. It is important to note that the new offence can still bite on non-UK organisations if there is a UK nexus, for example if some element of the fraud was carried out in the UK or the fraud targets victims in the UK.

Reasonable procedures

The section of the new Guidance that sets out procedures that organisations can put in place to prevent fraud is based on the same 'six principles' familiar from the previous Government guidance on other 'failure to prevent' offences. However, there are notable differences and changes of emphasis. The new Guidance offers a more detailed and structured set of procedural recommendations. It encourages businesses to draw on a broader array of resources, including the UK Corporate Governance Code, and the US Guidance on Corporate Compliance Programmes, relevant caselaw, and industry publications.

The Guidance reflects a more comprehensive and mature approach than we have seen from the previous guidance documents. This is perhaps to be expected in circumstances where law enforcement agencies have been grappling with what 'adequate' or 'reasonable' compliance procedures should look like since the earliest investigations under the failure to prevent bribery offence. The past 15 years have been a period of significant development in the way in which risk generally, and financial crime risk in particular, is managed within organisations, including the increased professionalisation of compliance as a specialised area of expertise.

The Guidance is advisory only and is not legally binding. Further, while it serves as a very useful starting point, the Guidance remains somewhat flexible – it does not provide a straightforward blueprint for implementation. It is expressly stated in the Guidance that *"departures from suggested procedures within the guidance will not automatically mean that an organisation does not have reasonable fraud prevention procedures"* and *"[e]qually, this guidance is not intended to provide a safe harbour: even strict compliance with the guidance will not necessarily amount to having reasonable procedures."* The Guidance is clear that organisations need to evaluate their own unique risk profile and develop bespoke, but proportionate, mitigation strategies in response.

Despite its inherent flexibility, the Guidance does offer an important insight into the approach that investigating authorities and prosecutors will take when, in the context of investigating the new offence, they assess whether reasonable procedures were in place. In practice, organisations attempting to rely on the defence who have not implemented the specific recommendations in the Guidance will need to be able to explain, with evidence, why they did not do so.

Further detail on the content of the Guidance is set out below, under the 'six principles'.

(1) Top level commitment

The new Guidance goes beyond previous guidance documents on this principle, offering greater detail on the practical steps and best practice for senior management, to help foster a culture where fraud is unacceptable. Some of the recommended practical steps include:

- Designating responsibility for horizon scanning for new fraud risks.
- Updating the board on fraud compliance as part of its ongoing oversight responsibilities.
- Actively articulating the business benefits of rejecting fraud and the consequences for individuals who breach the fraud policies.

Promoting an open culture for reporting fraud concerns is a central theme in the new Guidance, emphasising senior management's key role in driving ethical conduct. Senior management is expected to actively participate in anti-fraud initiatives and ensure that adequate training and resources are available to support fraud prevention.

(2) Risk assessment

The Guidance is clear that an organisation's fraud risk assessment is the bedrock on which 'reasonable procedures' are built. In a sign of the more mature approach taken in this Guidance, it acknowledges that it is not possible to anticipate all potential fraud risks but gives some guidance on how organisations should approach

their fraud risk assessments, including consideration of the 'fraud triangle'[2] . The Guidance notes that failing to carry out a risk assessment will "rarely be considered reasonable" and failure to review it periodically might mean that reasonable procedures were not in place at the relevant time.

(3) Proportionate risk-based fraud prevention procedures

This principle closely aligns with that in previous guidance documents – after completing a risk assessment, organisations should develop a fraud prevention plan tailored to the identified risks and to the scale and complexity of their organisation. An interesting addition to this principle that appears in the new Guidance is that *"[a]ny decision made not to implement procedures to prevent a specific risk should be documented, together with the name and position of the person who authorised that decision and reviewed as appropriate"* – guidance that will likely make organisations think carefully about whether it is reasonable for there to be no mitigating procedures in place for a particular risk.

(4) Due diligence

The actions of third parties outside the business can, as with other 'failure to prevent' offences, lead to corporate liability. However, the guidance on this principle is relatively sparse, advising only that organisations take a 'proportionate and risk-based approach.' In practice many organisations within the scope of the new offence will already have mature due diligence processes in place for employees and third-party service providers. Whilst the Guidance notes that merely applying existing procedures tailored to a different type of risk will not necessarily be an adequate response to tackle the risk of fraud, it only offers limited examples of best practice, such as using third-party tools and including compliance obligations in contracts with third parties.

Given the central role of third-party due diligence in any financial crime compliance programme it is surprising that the Guidance does not provide more detailed advice on this principle. Organisations may find it useful to consider the US Guidance on Corporate Compliance Programmes, which is referenced elsewhere in the Guidance and offers detailed insights on due diligence – including the importance of a risk-based integrated approach, effective controls and relationship management.

(5) Communication

This principle highlights the importance of communicating and embedding fraud prevention policies and training across the organisation. Notably, it includes a new section dedicated to whistleblowing – a development from previous guidance, in which whistleblowing was only briefly mentioned. This addition reflects the increasing focus on effective 'speak up' procedures and sets new expectations for whistleblowing programmes, even outside the regulated financial sector. This emphasis on whistleblowing will likely be welcomed by the SFO, which has advocated in recent times for financial incentives for whistleblowers.

(6) Monitoring and review

This principle advises organisations to continually monitor and refine their fraud detection and prevention measures, incorporating lessons from past investigations and whistleblowing incidents. While this aspect is familiar, the Guidance reflects an increasing emphasis on integrating technology and AI into these processes. Indeed, four of the six principles expressly refer to technology solutions for fraud prevention – reflecting not only developments in compliance practices but also the growing prominence and accessibility of advanced tools and AI. Prosecutors may increasingly consider the use of these technologies when evaluating not just the new offence, but all 'failure to prevent' offences. However, it is important to recognise that the effectiveness of these technologies hinges on accurate data, thoughtful implementation, and ongoing human oversight. Without these elements, these technologies risk becoming more of a compliance checkbox than meaningful prevention measures.

Interaction with Existing Procedures

The Guidance recognises that many large organisations already have compliance processes that could help reduce fraud risks – such as those for financial reporting. While some of these procedures can be adapted to prevent duplication, the Guidance warns that simply relying on them without proper consideration of whether they are fit

[2] The fraud triangle is a framework commonly used to explain the reason behind an individual's decision to commit fraud. It sets out three components that are understood to contribute to an individual's decision to commit fraud: (1) opportunity, (2) motive, and (3) rationalisation.

for purpose in the context of the new offence is unlikely to be sufficient.

For example, organisations should consider whether their current anti-fraud procedures, which may focus on preventing fraud against the company (ie. 'inward fraud', where the company is the victim) respond appropriately to the risk of fraud being committed for the company's benefit ('outward fraud' – which is the focus of the new offence). Meeting this new standard may require the development of targeted new policies and procedures.

The new Guidance will also shape expectations for procedures that are in place to prevent bribery and facilitation of tax evasion. The Government guidance on these offences and their procedures – issued 14 and seven years ago respectively – could now be said to be somewhat out of date in terms of best practice for financial crime compliance. Given the more recent and detailed nature of this Guidance, law enforcement agencies that are handling cases under the older failure to prevent offences may well look to it for additional guidance. As such, companies would be well advised to consider this Guidance as part of a refresh of their financial crime procedures more generally.

Enforcement outlook

The SFO appears eager to deploy the new offence and make an example of corporate offenders, but any enforcement actions are likely to take time. SFO investigations are notoriously lengthy, despite almost every incoming SFO Director saying that they will speed them up, and the offence will only apply to conduct occurring after 1 September 2025. In the meantime, the hypothetical case studies in the Guidance offer some insights into the types of scenarios that could trigger investigations. Notably, eight of these case studies focus on ESG-related fraud and the offence's extraterritorial reach, signalling that these are areas of interest for law enforcement – although of course they are in fact likely to be some of the hardest to investigate, let alone prosecute.

The Guidance also suggests that enforcement actions in relation to the new offence, such as prosecutions and Deferred Prosecution Agreements (DPAs), could, over time, shed light on what constitutes reasonable and proportionate anti-fraud measures. However, whilst this is possible, it is unrealistic to expect this to happen. The failure to prevent bribery offence came into force in July 2011, but prosecutions and DPAs for that offence have, to date, provided very little clarity on the scope of the 'adequate procedures' defence in that legislation. For now, the responsibility lies with companies and their advisers to carefully review the Guidance and anticipate what prosecutors and the courts might deem reasonable in the context of their business.

What should organisations do now?

Organisations must act swiftly to ensure reasonable fraud prevention procedures are in place before the new offence takes effect on 1 September 2025. Whilst nearly ten months may seem like ample time, the timetable remains challenging, particularly for large businesses with numerous interested stakeholders.

The new Guidance sets out clear, actionable expectations for fraud prevention procedures. The first step should be to carry out a **comprehensive risk assessment** to identify the unique fraud risks specific to the business and its sector. This includes understanding who the business's 'associated persons' are and what might drive them to commit fraud. This risk assessment is the foundation of any effective fraud prevention compliance framework. Once these risks are identified, **tailored policies and procedures should be implemented** to address them, followed by communication and training to embed these practices across the business. All these measures need to be in place by the 1 September 2025 deadline to maximise their protective effect – so organisations should start their risk assessments soon.

Additionally, it is important to fully document the steps taken in response to the Guidance, including the considerations and decisions made about enhancements to policies and procedures. This documentation will serve as crucial evidence and put an organisation in the best position possible if it ever needs to rely on the reasonable procedures defence.

CONTACT

JONATHAN COTTON
PARTNER
T:+44 (0)20 7090 4090
E: Jonathan.Cotton@slaughterandmay.com

ELLA WILLIAMS
SENIOR COUNSEL
T: +44 (0)20 7090 5340
E: Ella.Williams @Slaughterandmay.com

ORLA FOX
SENIOR PROFESSIONAL SUPPORT LAWYER
T: +44 (0)20 7090 3814
E: ORLA.FOX@SLAUGHTERANDMAY.COM

London
T +44 (0)20 7600 1200
F +44 (0)20 7090 5000

Brussels
T +32 (0)2 737 94 00
F +32 (0)2 737 94 01

Hong Kong
T +852 2521 0551
F +852 2845 2125

Beijing
T +86 10 5965 0600
F +86 10 5965 0650