

Introduction

On 6 November 2024, the UK Government released its much-anticipated Economic Crime and Corporate Transparency Act 2023: Guidance to Organisations on the Offence of Failure to Prevent Fraud (Guidance).¹ This provides guidance on the steps companies should take to implement reasonable procedures to prevent fraud and avail themselves of a defence to the failure to prevent fraud offence (FTPFO). The clock is now ticking for businesses to conduct risk assessments and have an appropriate compliance framework in place before the FTPFO comes into force on 1 September 2025. We have provided some high-level pointers on the steps organisations should take to prepare below.

We are holding two events that you can sign up to for further assistance:

- **Webinar providing an overview of the “failure to prevent fraud” offence on 29 January 2025 from 1 p.m. – 2 p.m.**
In this session, we will delve into the provisions of the Economic Crime and Corporate Transparency Act (ECCTA), examine the types of conduct it covers and discuss the changes to corporate criminal liability. To register your interest, please click [here](#).
- **In-person roundtable at Squire Patton Boggs London offices on 12 February 2025 from 9 a.m. – 10:15 a.m.**
(with breakfast beforehand). We will moderate a roundtable discussion with in-scope organisations, looking at practical approaches to conducting risk assessments and establishing effective “failure to prevent” compliance frameworks having regard to the guidance. To register your interest, please click [here](#); this event will have limited seating.

Failure to Prevent Fraud Offence

We provided an overview of the FTPFO in our [September 2024 alert](#). In summary, large organisations, wherever located, can be held criminally liable if a fraud offence is committed by an “associated person” for, or on behalf of the organisation with the intention of benefiting the organisation or its clients. Associated persons include employees, agents, subsidiaries and any individuals or entities providing services on behalf of the company or its subsidiaries. The underlying misconduct covers a wide range of economic crime. While this underlying misconduct must have a UK nexus to give rise to liability, this has been interpreted broadly.

Companies can defend themselves against allegations by demonstrating that they had “reasonable fraud prevention” procedures in place at the time of the alleged misconduct.

The Guidance outlines critical considerations for implementing such procedures, which we explore in detail below.

If a company is found guilty of failing to prevent fraud, it may face significant financial penalties.

The Guidance on Reasonable Fraud Prevention Measures

The structure of the Guidance will be familiar to businesses who have implemented compliance regimes for other “failure to prevent” offences, e.g., under the UK Bribery Act 2010 (UKBA”), as it follows a similar structure by reference to the six fundamental principles that businesses should apply when implementing appropriate controls: top-level commitment; risk assessment; proportionate risk-based prevention procedures; due diligence; communication (including training) and monitoring and review.

However, there are critical differences that must be considered when determining whether the FTPFO applies to an organisation, the scope of that liability, the potential criminal conduct that could give rise to liability and which associated persons pose the greatest risk. Accordingly, companies cannot just rely upon the risk assessments and compliance measures that they have in place for other failure to prevent offences, and should tailor their compliance to address the specific requirements of the FTPFO.

We summarise key elements of the Guidance below.

Top Level Commitment

The responsibility for preventing and detecting fraud rests with the organisation’s senior management and executives. Senior management is expected to play an active role in fraud prevention, promoting a culture of openness and trust that encourages employees to report suspected fraud or other forms of misconduct. This includes:

- Communication and endorsement of the organisation’s position on preventing fraud
- Designing and implementing clear governance across the organisation
- Committing to allocating a reasonable and proportionate budget for training and resourcing of the fraud prevention plan
- Leading by example and fostering an open culture where employees feel empowered to “speak up” and report suspected fraud, or other forms of misconduct

¹ Home Office, Economic Crime and Corporate Transparency Act 2023: [Guidance to Organisations on the Offence of Failure to Prevent Fraud](#) (6 November 2024).

Risk Assessment

Companies should conduct economic crime risk assessments, which include the risk that associated persons may commit fraud offences covered under the new offence. The Guidance highlights that risk assessments should be “dynamic, documented and kept under regular review” and that “nominated risk owners” in the organisation should take responsibility for developing the risk typologies. The Guidance recommends developing typologies of risks using the fraud triangle (opportunity, motive and rationalisation).

Proportionate Risk-Based Prevention Procedures

Businesses must use their risk assessment to inform the fraud prevention plan and control framework. The plan must align with the identified risks and be proportionate to their potential impact and the nature, scale and complexity of the company’s activities. The Guidance emphasises that organisations should:

- Begin by evaluating their current compliance policies and procedures to determine whether they adequately address the fraud risks identified during the risk assessment and address any gaps.
- Consider any sector-specific guidance that helps set standards or clarify requirements. Adopt procedures customised to the company’s unique risks and avoid generic or “template” procedures.
- Assign responsibility for assessing the effectiveness of fraud prevention plans to employees within the organisation who were not involved in designing the procedure.

Due Diligence

Organisations should adopt a risk-based approach to due diligence, ensuring procedures are thoughtfully tailored to address the specific risks of the offence. In particular, companies should:

- Consider whether existing processes to detect and prevent fraud are adequate, and enhance them where necessary
- Integrate rigorous fraud prevention measures following a merger or acquisition
- Conduct thorough due diligence on associated persons
- Leverage appropriate technologies, including third-party tools

Communication (Including Training)

The Guidance emphasises the importance of clearly communicating the commitment to fraud prevention across all levels of the organisation and integrating this message into existing policies to reinforce its significance. Employees must receive up-to-date training on fraud prevention policies and procedures and the organisation’s whistleblowing procedures.

Monitoring And Review

Companies are expected to routinely assess and update their fraud detection, as well as prevention measures and monitor their effectiveness. Reviews should draw on findings from previous internal fraud investigations, whistleblower reports and industry-specific guidance. The Guidance also emphasises the potential role of using advanced technologies, such as data analytics tools and artificial intelligence, in strengthening fraud detection capabilities.

Next Steps

Organisations should use the next nine months to establish robust fraud prevention procedures before the offence comes into force on 1 September 2025. As per the Guidance, while organisations do not need to duplicate existing financial crime measures, they must not simply rely on current procedures. A dedicated fraud-specific risk assessment is crucial to ensure adequate preparation. We recommend that organisations take the opportunity to prepare and implement the following next steps:

- **Conduct a risk assessment** – Perform a thorough risk assessment to identify gaps and prioritise areas of risk.
- **Develop a tailored, proportionate plan** – Create a well-structured and proportionate fraud prevention plan that addresses the identified risks directly.
- **Evaluate current policies and procedures** – Examine existing policies and procedures to ensure they are effective.
- **Enhance procedures and address gaps** – Regularly assess and update fraud prevention procedures to mitigate the organisation’s risks. Update risk assessments and controls in line with changes in the business.
- **Communicate commitment** – Communicate the company’s dedication to fraud prevention across all levels of the organisation.
- **Deliver comprehensive training** – Provide all employees with relevant training and implement additional sessions to address identified knowledge gaps.
- **Establish whistleblowing channels** – Maintain robust and accessible whistleblowing mechanisms to encourage reporting of potential and actual misconduct.
- **Seek legal expertise** – Consult legal advisors to understand the complexities of the legal framework and compliance requirements.

Contacts



Hannah Laming

Partner, London
T +44 20 7655 1682
E hannah.laming@squirepb.com



Malak Abbas

Associate, London/Dubai
T + 44 207 655 1508
E malak.abbas@squirepb.com