



Failure to prevent fraud: what should you be doing before September?



By Andrew Reeves (UK), Stuart Neely (UK), Katie Stephen (UK), Hannah McAslan-Schaaf (UK), David Harris (UK), Emily Smith & Claudia Van Gruisen on April 11, 2025

With less than five months to go until the new UK failure to prevent fraud offence comes into force on 1 September 2025, many organisations are conducting risk assessments and enhancing anti-fraud policies and procedures with a view to preventing fraud and providing themselves with a defence should this be necessary.

The new offence will apply to organisations wherever they are located (including outside the UK), where a fraud is committed which has some nexus to the UK. The only defence for an organisation will be to have “reasonable procedures” in place to prevent fraud. More details on the new offence, including the underlying fraud offences covered, are set out [here](#).

In a recent speech the SFO Director Nick Ephgrave emphasised that the SFO is looking to prosecute the offence, and noted that organisations

should ensure their procedures are in place by September:

“Come September, if they haven’t sorted themselves out, we’re coming after them. That’s the message I’ll be delivering...I’m very, very keen to prosecute someone for that offence. We can’t sit with the statute books gathering dust, someone needs to feel the bite.”

Whilst, in practice, many organisations will (and should) be continuing to enhance their policies and procedures on an ongoing basis, it is important that organisations have taken significant steps ahead of September to implement “reasonable procedures”, and that there is a clear plan for further review (and a process for making enhancements, should those be required) in future.

We will be publishing a series of articles on key steps to take ahead of September. In this article we explore one of the first steps in preparing for the new offence: conducting a risk assessment.

Part 1: Risk assessments

As the Home Office’s November 2024 guidance (the **HO Guidance**) and UK Finance’s February 2025 guidance (the **UKF Guidance**) (together the **Guidance**) acknowledge, organisations (particularly those in the financial services and other regulated sectors) may already have existing risk assessment frameworks in place that can be adapted to address the risks presented by the new offence.

Our expectation is that conducting a failure to prevent fraud risk assessment will take some time – the Home Office issued an impact assessment (see [here](#)) in November 2022 which estimated that risk assessments should take organisations between c.100-130 hours to prepare.

There are a number of considerations to work through when an

organisation is assessing its approach to risk assessments. We explore each of these below.

1. Deciding who will conduct and oversee the risk assessment

Jurisdictional scope: the new offence will apply to any organisation and could arise where a fraud offence is committed with a connection to the UK (e.g. because a meeting is held or communication is made in the UK) or where there are victims in the UK (which could include investors and / or counterparties) or, in some cases, where there is a gain or loss in the UK. This means that whether an organisation is subject to the offence will vary depending on the specific circumstances in which the fraud takes place (and so could shift from transaction to transaction, or as its investor profile changes). In addition to the jurisdictional scope question, organisations need to decide whether to approach implementation on a global or local scale. -Multinational organisations may choose to conduct risk assessments and enhance fraud procedures on a global basis (although in the short term it may make sense to focus efforts on UK entities and other entities with a UK nexus).

Ownership: it is rare that a single function can effectively conduct the failure to prevent fraud risk assessment or enhance / implement the requisite procedures to ensure compliance with the new offence on its own. Input from stakeholders across the organisation is likely to be required to fully understand the scenarios in which fraud risks could arise in practice. We have helped clients put in place cross-functional working groups to obtain input from a variety of different business units including finance, marketing, sales, procurement, legal, sustainability, ethics/compliance and internal audit.

Oversight by senior management: the Guidance suggests it may be appropriate that some level of approval of the risk assessment should be given by senior management/the Board and that there should be

designated responsibility *for horizon scanning for new fraud risks* and approving *the assessment of risk*. We would recommend that the approach taken in conducting a risk assessment is agreed at a senior level at the outset, with appropriate consideration given to resource allocation, coordination (e.g. via a working group) and reporting. There should be a specific budget and resources for undertaking the risk assessment as well as making relevant enhancements to procedures.

Level of external input: it is worth considering the level of support required from external providers to undertake risk assessment(s). Although much of the knowledge required to conduct the risk assessment will be held internally, many organisations will need some level of external legal support including to work through the details of the offences and how they can be committed in practice, navigating some of the core scoping questions such as those relating to the definition of associated persons and questions of territoriality, and benchmarking against peer organisations.

2. Understanding the relevant risk assessments already in place; and what they do and do not cover

Most organisations (particularly those in the financial services and other regulated sectors) have some kind of risk assessment in place that covers fraud. Many of these existing risk assessments focus on cases where the organisation is a victim of fraud (i.e. “inward fraud”) rather than addressing fraud committed by Associated Persons for the benefit of the organisation or its clients (i.e. “outward fraud”). Appreciating this distinction is essential in terms of ensuring the risk assessment is fit for purpose.

3. Assessing the likelihood of the underlying fraud offences arising

It is crucial that those undertaking the risk assessment and enhancing anti-fraud procedures understand the underlying offences in sufficient

detail. The offences are complex (much more so than, for example, those under the UK Bribery Act) and often the precise conduct covered by the offence is not obvious from the shorthand description set out in the relevant legislation. Further, there are numerous “grey areas” around whether certain conduct would meet the relevant standard of dishonesty (a defining characteristic of nearly all of the underlying offences) which need to be thought through.

Given these challenges, many clients have found it useful to break down each offence into its constituent elements and to bring these to life with examples of how each offence could potentially be committed in practice in their sector (and, as set out below, in each different business unit or support function or by their associated persons).

Once the underlying offences are fully understood by those participating in the risk assessment process, it is then important to assess how they could arise.

The Guidance suggests as a starting point identifying different types of Associated Person and then for “nominated risk owners” to consider circumstances in which those associated person might attempt fraud (and whether there are particular types of fraud offence, e.g. false accounting or abuse of position which are more likely to be committed by particular types of Associated Persons).

A strategy we have seen work well to put structure around this is to have each business head lead an appropriate discussion about the offences within their function and this may be facilitated by an internal questionnaire. The business head can then feed back to the working group those scenarios which have been identified as risk areas and any relevant controls. This enables the organisation to build up one document setting out risk areas across the business for each underlying offence and will also help to promote consistency across different business lines and

functions. An element of cross fertilisation with different internal teams learning from each other's examples can also be helpful.

For organisations starting their risk assessments now, it may make sense to determine, and focus in the first instance on, areas of highest risk in order to identify priority programme enhancements (see below).

4. Conducting a "gap analysis" to assess what policies and procedures are already in place and identify any areas for enhancement

It is important to understand the extent to which existing policies or procedures (whether fraud specific or otherwise) can be adapted or supplemented. Many organisations will already have in place policies, procedures and controls that can be leveraged (e.g. third-party due diligence and monitoring processes related to bribery and corruption and controls around financial reporting and approval of marketing materials).

Many clients have found it useful to identify, in relation to each offence and the scenarios which have been identified, relevant controls that are in place. Those controls can then be reviewed to determine whether there are any "gaps" and to identify where enhancements may be required. An enhancement and prioritisation plan can then be drawn up based on the output of this work. This exercise is also useful in drawing together all the relevant internal anti-fraud procedures so that there is a central record of these that could be deployed as part of any defence strategy if needed.

5. Producing a written risk assessment and agreeing when it will be reconsidered

Whilst the primary purpose of anti-fraud procedures is, of course, to stop fraud happening in the first place, it is also crucial that an organisation can defend itself if allegations of fraud are raised and it is facing a criminal investigation (or seeking to persuade criminal authorities not to

investigate) or alternatively a regulatory investigation. This means the organisation's procedures, including the risk assessment, need to be documented carefully.

To defend procedures effectively requires contemporaneous documentation of the decisions made and steps taken in conducting a risk assessment, including the rationale for those decisions. For example, where an offence arises in an area of a business which was deprioritised in light of the risk assessment, following a risk-based approach it will be important to be able to provide contemporaneous evidence of the rationale for that decision. This is particularly important where the organisation will not have finalised its anti-fraud procedures by September.

How often should the risk assessment be refreshed? The guidance states that the risk assessment should be dynamic and kept under regular review, either annually or bi-annually. Risk assessments should be refreshed in the interim as the business (and risks faced by the business) change – and in light of any fraud issues identified either internally or where knowledge of peer experience is available.

We are helping various organisations prepare for this change: if you would like to discuss how we can help, please get in touch.

Global Regulation Tomorrow

Published by

