PWYLLGOR ARCHWILIO A SICRWYDD RISG
AUDIT AND RISK ASSURANCE COMMITTEE

DYDDIAD Y CYFARFOD: **DATE OF MEETING:**	10 December 2024
TEITL YR ADRODDIAD: **TITLE OF REPORT:**	Economic Crime and Corporate Transparency Act 2023: Guidance to organisations on the offence of failure to prevent fraud
CYFARWYDDWR ARWEINIOL: **LEAD DIRECTOR:**	Huw Thomas, Director of Finance
SWYDDOG ADRODD: **REPORTING OFFICER:**	Ben Rees, Head of Counter Fraud

Pwrpas yr Adroddiad (dewiswch fel yn addas) **Purpose of the Report** (select as appropriate)
Er Sicrwydd/For Assurance

ADRODDIAD SCAA
SBAR REPORT

Sefyllfa / Situation

The Economic Crime and Corporate Transparency Act 2023 created the new corporate offence of failure to prevent fraud. Under the offence, *an organisation may be criminally liable where an employee, agent, subsidiary, or other 'associated person', commits a fraud intending to benefit the organisation and the organisation did not have reasonable fraud prevention procedures in place*.

The Home Office has now issued guidance (attached as Appendix 1) to organisations regarding the offence, and sets out the procedures that relevant bodies can put in place to prevent persons associated with them from committing fraud offences. Ultimately, only courts can determine whether a relevant body has reasonable prevention procedures in place, taking into account the facts and circumstances of the case. The offence will come into effect on 1 September 2025.

The Audit and Risk Assurance Committee is asked to consider the policies and procedures in place to counter fraud within the Health Board and take assurance that these are adequate to show that reasonable measures are in place to prevent the new offence of failure to prevent fraud.

Cefndir / Background

The Economic Crime and Corporate Transparency Act 2023 created the new corporate offence of failure to prevent fraud, following a Law Commission paper in June 2022 that sought ways to improve the law to ensure that corporations are effectively held to account for committing serious crimes.

Under the offence, *an organisation may be criminally liable where an employee, agent, subsidiary, or other 'associated person', commits a fraud intending to benefit the organisation and the organisation did not have reasonable fraud prevention procedures in place*.

It does not need to be demonstrated that directors or senior managers ordered or knew about the fraud. The offence sits alongside existing law; for example, the person who committed the fraud may be prosecuted individually for that fraud, while the organisation may be prosecuted for failing to prevent it.

The offence applies to large[1], incorporated[2] bodies and partnerships across all sectors of the economy.

The offence applies to a number of specific fraud offences, referred to as 'base fraud' offences in the guidance. Aiding, abetting, counselling or procuring the commission of any of the listed offences would also qualify as a base offence. Relevant organisations can be prosecuted if the associated person's conduct constitutes a base fraud offence, even if the associated person is prosecuted for an alternative offence or is not prosecuted at all. The types of fraud covered by the offence are:

- Fraud offences under section 1 of the Fraud Act 20069 including:
  - Fraud by false representation (section 2 Fraud Act 2006)
  - Fraud by failing to disclose information (section 3 Fraud Act 2006)
  - Fraud by abuse of position (section 4 Fraud Act 2006)
- Participation in a fraudulent business (section 9, Fraud Act 2006)
- Obtaining services dishonestly (section 11 Fraud Act 2006)
- Cheating the public revenue (common law)
- False accounting (section 17 Theft Act 1968)
- False statements by company directors (section 19 Theft Act 1968)
- Fraudulent trading (section 993 Companies Act 2006).

The base fraud offence is committed by a 'person associated with the relevant body'. An employee, an agent or a subsidiary of the relevant body is automatically an 'associated person' for the purposes of this offence. A person who provides services[3] for or on behalf of the relevant body is also an associated person while they are providing those services. The corporate offences can only take place if the person commits a base fraud whilst acting in the capacity of a person associated with the relevant body. Fraud that takes place outside this capacity, for example in the person's private life, does not give rise to corporate liability.

The issue of who is intended to benefit from the underlying fraud is key to determining whether a relevant organisation can be held accountable for the offence of failure to prevent fraud. An organisation does not need to actually receive any benefit for the offence to apply - since the fraud offence can be complete before any gain is received. It is enough that the organisation was intended to be the beneficiary. The intention to benefit the organisation does not have to be the sole or dominant motivation for the fraud. The offence can apply where a fraudster's primary motivation was to benefit themselves, but where their actions will also benefit the organisation. The relevant organisation is not liable if it is a victim or intended victim of a fraud that was intended to benefit the organisation's clients.

[1] Defined as meeting two or three out of the following criteria

- More than 250 employees
- More than £36 million turnover
- More than £18 million in total assets

[2] Including by statute

[3] Providing services does not include providing goods. It also does not include persons providing services t**o** the relevant body.

The guidance states that the fraud prevention framework put in place by relevant organisations to demonstrate they have reasonable procedures in place to prevent fraud should be informed by the following six principles:

- Top level commitment
- Risk assessment
- Proportionate risk-based prevention procedures
- Due diligence
- Communication (including training)
- Monitoring and review

The guidance recognises that public sector organisations are already required to implement the recommendations of the Government Functional Standards 013 - Counter Fraud (GovS 013). In addition, NHS bodies in Wales must implement anti-fraud, bribery, and corruption measures in accordance with Government Directions on Counter Fraud Measures and the service agreement under section 83 of the Government of Wales Act 2006. However, it suggests that, where applicable, the procedures should be adapted to take account of the new offence.

Asesiad / Assessment

The Head of Local Counter Fraud has undertaken a self-assessment of the measures in place within Hywel Dda University Health Board. It is their view that the Health Board can demonstrate reasonable fraud prevention procedures in the context of this guidance via existing counter fraud arrangements within the Health Board and wider NHS. These arrangements include, but are not limited to, having in place:

- An annual Counter Fraud Workplan and Strategy, which is aligned to Government Functional Standard 013 Counter Fraud - NHS Requirements, with which the Health Board is bound to comply.
- An awareness programme, which includes a mandatory Anti-Fraud, Bribery and Corruption e-learning package.
- A Counter Fraud, Bribery and Corruption Policy.
- A Standards of Behaviour Policy, which includes specific reference to fraud, bribery and corruption and the need to declare any conflicts of interest.
- A Risk Management Strategy and Policy.
- An annual Internal Audit Workplan.

Government Functional Standard 013 - Counter Fraud, sets the expectations for the management of fraud, bribery, and corruption risk in government organisations. The NHS is one such organisation which is required to comply with these standards, which will assist in ensuring the existing procedures remain robust for preventing fraud, bribery, and corruption.

Any specific actions around continuing compliance will be included in the Health Board's governance arrangements, which will include the Counter Fraud Work Plan and annual Internal Audit Plan.

The introduction of this legislation and accompanying guidance will only strengthen the fraud prevention efforts of the organisation by creating a business environment with an increased anti-fraud culture.

The following specific areas in the guidance are highlighted for comment:

Who commits the fraud
It is noted that those within the organisation's supply chain are not associated persons unless they are providing services on behalf of the relevant body; however, existing controls, including supply chain due diligence, contractual controls and relevant frameworks will contribute to mitigating the risk of fraud, bribery and corruption and assist in demonstrating defence of reasonable fraud prevention procedures.

Who benefits and how
The failure to prevent fraud offence is a strict liability offence which can only be committed by corporations. Any individuals involved in wrongdoing may, of course, be prosecuted under existing legislation as individuals for their own fraud offences or for encouraging or assisting fraud. A key difference of the failure to prevent fraud offence is that a company will be exempt from prosecution if they are, or were intended to be, a victim of the fraud. This means a company will not have committed an offence itself where an associate of the organisation commits a fraud for their own benefit rather than for the benefit of the company.

However, it is recognised that there is a responsibility on the organisation to reduce fraud, bribery, and corruption to an absolute minimum. This is currently achieved by a programme of Counter Fraud work which Hywel Dda University Health Board has adopted and implements via a top-down approach to reducing fraud, bribery, and corruption to an absolute minimum.

Defence of reasonable fraud prevention procedures
The only way for an organisation to avoid prosecution, or conviction, will be if it can prove that it had in place reasonable fraud prevention procedures or that it was not reasonable to have any such procedures in place (e.g. if the risk of fraud being committed was extremely low).

The use of the broader 'reasonable procedures' wording, raises the question over how it could be reasonable for a large organisation with deep pockets not to have fraud prevention procedures in place. As with the failure to prevent bribery guidance, these prevention principles are deliberately flexible so they can be tailored to the circumstances of each organisation. Any procedures to prevent fraud need to be proportionate to the risk faced by the individual organisation. The principles mentioned underpin current working practices and the Health Board's Counter Fraud Strategy.

Fraud Risk, Prevention and Due Diligence
In line with Government Functional Standard 013 Counter Fraud - NHS Requirements, there is a requirement that the NHS Local Counter Fraud Specialist has in place an annual work plan that covers both reactive and proactive work. This includes having in place a strategy to assess, evaluate and treat Fraud Risk in line with the Health Board's Policy. This will include the requirement to undertake pro-active exercises to test and strengthen existing controls and to identify others.

The Health Board's position
Having considered the Health Board's internal systems and procedures in line with the fraud prevention principles, the following arrangements are in place. Some suggestions for strengthening are also highlighted in italics:

- Set the right tone - continue to demonstrate HDdUHB's commitment to preventing fraud with clear internal communications and resources for employees as well as ensuring the correct functional support is in place for decision making.
- Conduct impact assessments as to where fraud risks originate - continue to measure risks in line with the Health Board's Risk Management Strategy and Framework. The undertaking

of Fraud Risks assessments plays a key role in the Counter Fraud Strategy and Annual Work plan.
It is recommended that a formal risk assessment be undertaken by Counter Fraud to appropriately assess and report on both existing and future controls required to mitigate the risk going forward.

- Implement training - at present, the Health Board requires that all employees undertake manual e-learning with respect to countering fraud in the NHS. This is further strengthened by Counter Fraud activity around inform and involve. This includes, providing specific training to high-risk groups within the organisation.
- *Engage with NWSSP Procurement to update third-party contracts - ensure they are up to date with market standards and that the new offence is included when it comes into force.*
- Review HDdUHB's Financial Policies and Procedures to ensure compliance against the guidance. This will be a rolling review, which again, is currently part of the Counter Fraud annual plan.
- Ensure that the all Wales 'Raising a Concern' policy and internal systems allow instances of fraud to be identified by encouraging reporting and clearly outlining the types of practices that might capture this new offence.

Argymhelliad / Recommendation

The Audit and Risk Assurance Committee is asked to **CONSIDER** the policies and procedures in place to counter fraud within the Health Board and **TAKE ASSURANCE** that these are adequate to show that reasonable measures are in place to prevent the new offence of failure to prevent fraud.

Amcanion: (rhaid cwblhau) **Objectives: (must be completed)**	
Committee ToR Reference: Cyfeirnod Cylch Gorchwyl y Pwyllgor:	3.2 In particular, the Committee will review the adequacy of: 3.2.4 the policies and procedures for all work related to fraud and corruption as set out in National Assembly for Wales Directions and as required by the Counter Fraud and Security Management Service.
Cyfeirnod Cofrestr Risg Datix a Sgôr Cyfredol: Datix Risk Register Reference and Score:	Not applicable
Parthau Ansawdd: Domains of Quality Quality and Engagement Act (sharepoint.com)	3. Effective 4. Efficient
Galluogwyr Ansawdd: Enablers of Quality: Quality and Engagement Act (sharepoint.com)	4. Learning, improvement and research
Amcanion Strategol y BIP: UHB Strategic Objectives:	3. Striving to deliver and develop excellent services 6. Sustainable use of resources

Amcanion Cynllunio Planning Objectives	Not Applicable
Amcanion Llesiant BIP: UHB Well-being Objectives: Hyperlink to HDdUHB Well-being Objectives Annual Report 2021-2022	10. Not Applicable

Gwybodaeth Ychwanegol: Further Information:	
Ar sail tystiolaeth: Evidence Base:	Counter Fraud Workplan 2024/25 Economic Crime and Corporate Transparency Act | The Law Society Economic Crime and Corporate Transparency Act 2023: Who is an Associated Person for the Failure to Prevent Fraud Offence? | Herbert Smith Freehills | Global law firm Economic Crime and Corporate Transparency Act 2023 - Mountford Chambers - London Barristers Chambers New UK 'failure to prevent' fraud corporate criminal offence published - A&O Shearman
Rhestr Termau: Glossary of Terms:	Contained within the body of the report
Partïon / Pwyllgorau â ymgynhorwyd ymlaen llaw y Pwyllgor Archwilio a Sicrwydd Risg Parties / Committees consulted prior to Audit and Risk Assurance Committee:	Not applicable

Effaith: (rhaid cwblhau) Impact: (must be completed)	
Ariannol / Gwerth am Arian: Financial / Service:	Failure to prevent the offence could lead to a financial penalty.
Ansawdd / Gofal Claf: Quality / Patient Care:	Not applicable
Gweithlu: Workforce:	Not applicable
Risg: Risk:	The document sets out how the risks will be minimised.
Cyfreithiol: Legal:	Failure to prevent the offence could lead to prosecution.
Enw Da: Reputational:	Failure to prevent the offence could lead to reputational damage.
Gyfrinachedd: Privacy:	Not applicable
Cydraddoldeb: Equality:	Not applicable

Home Office

Economic Crime and Corporate Transparency Act 2023:

Guidance to organisations on the offence of failure to prevent fraud.

November 2024

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at public.enquiries@homeoffice.gov.uk.

Contents

Chapter 1: Introduction

1.1 Background and aim of the legislation

The Law Commission published a paper[1] in June 2022 examining options to improve the law to ensure that corporations are effectively held to account for committing serious crimes. This paper considered the creation of a new offence of failure to prevent fraud. This offence was created by the Economic Crime and Corporate Transparency Act 2023[2].

Under the offence, an organisation may be criminally liable where an employee, agent, subsidiary, or other "associated person", commits a fraud intending to benefit the organisation and the organisation did not have reasonable fraud prevention procedures in place. In certain circumstances, the offence will also apply where the fraud offence is committed with the intention of benefitting a client of the organisation. It does not need to be demonstrated that directors or senior managers ordered or knew about the fraud.

The offence sits alongside existing law; for example, the person who committed the fraud may be prosecuted individually for that fraud, while the organisation may be prosecuted for failing to prevent it.

The offence will make it easier to hold organisations to account for fraud committed by employees, or other associated persons, which may benefit the organisation, or, in certain circumstances, their clients. The offence will also encourage more organisations to implement or improve prevention procedures, driving a major shift in corporate culture to help prevent fraud.

The offence applies to large organisations[3] only and applies across the UK[4].

Although the offence of failure to prevent fraud applies only to large organisations, the principles outlined in this guidance represent good practice and may be helpful for smaller organisations.

[1] "Corporate Criminal Liability: an options paper", Law Commission, 10/06/2022, Corporate Criminal Liability - Law Commission

[2] Economic Crime and Corporate Transparency Act 2023 (legislation.gov.uk). The Economic Crime and Corporate Transparency Act 2023 also introduced amendments to the identification doctrine for economic crimes (sections 196-198). These amendments are not considered further in this guidance, but we recommend that organisations familiarise themselves with them.

[3] Note further comments on subsidiaries in 2.1 and 2.3.

[4] Note also 2.5 on territoriality.

1.2 Purpose of the guidance

This guidance is written under section 204 of the Economic Crime and Corporate Transparency Act 2023. This guidance sets out procedures that relevant bodies can put in place to prevent persons associated with them from committing fraud offences.
In line with the requirements of section 204, the Home Office has consulted the Scottish Government and Department of Justice in Northern Ireland on the content of this guidance.

While legislation is binding, this guidance is advisory. Moreover, the guidance is not a substitute for reading the legislation or obtaining professional legal advice.

This document provides an overview of the offence, illustrated by some theoretical examples in different contexts. It describes the general principles for organisations in developing or enhancing procedures to prevent fraud. When a court is considering a case, adherence to these principles will be taken into account. Each section includes examples of good practice, but, given the large range of organisations subject to the offence, the guidance cannot be prescriptive about all possible scenarios.

As some organisations in scope of the offence are also subject to other legislation (for example, financial, environmental or health and safety regulations), the guidance discusses how they should approach any potential overlap between the offence and existing regulatory requirements.

Departures from suggested procedures within the guidance will not automatically mean that an organisation does not have reasonable fraud prevention procedures, as different prevention procedures may also be considered reasonable by a court. Equally, this guidance is not intended to provide a safe harbour: even strict compliance with the guidance will not necessarily amount to having reasonable procedures where the relevant body faces particular risks arising from the unique facts of its own business that have not been addressed.

The onus will remain on the relevant organisation, where it seeks to rely on the defence, to prove that it had reasonable prevention procedures in place (or that it was unreasonable to expect it to have such procedures). In accordance with established case law, the standard of proof is the balance of probabilities. Ultimately only the courts can determine whether a relevant body has reasonable prevention procedures in place to prevent fraud in the context of a particular case, taking into account the facts and circumstances of that case.

1.3 Implementation Period

The offence will come into effect nine months after the publication of this guidance, to allow organisations to develop and implement their fraud prevention procedures.

1.4 Sector specific guidance

Individual sectors of the economy may choose to develop sector-specific guidance to provide more detail on prevention measures commensurate to the specific risks in that sector. However, there is no mechanism in the Act for statutory guidance to be issued by representative or membership bodies and therefore any sector-specific guidance will be advisory only. For sectoral guidance to be effective, it will need to be aligned with this guidance and the intent of the legislation, as well as endorsed by appropriate industry bodies. If there is a conflict between sector-specific guidance and this guidance, this guidance will take priority.

Chapter 2: Overview of the Offence

This section summarises the offence and when it applies. **However, organisations cannot rely on this alone and should take legal advice on how the offence affects them.**

The offence will hold organisations to account for fraud committed by their employees, agents, subsidiaries or other "associated persons" who provide services for or on behalf of the organisation, **where the fraud was committed with the intention of benefiting the organisation or their clients.** It does not need to be demonstrated that the organisation's senior managers or directors ordered or knew about the fraud.

The offence will *not* extend to *individual* liability for persons within the organisations who may have failed to prevent the fraudulent behaviour. However, this does not preclude the employee or agent who committed the base fraud, or anyone who encouraged or assisted them, being prosecuted for the base fraud in addition to the corporate being prosecuted for failing to prevent it.

The offence is set out in sections 199-206 and Schedule 13 of the Economic Crime and Corporate Transparency Act 2023. See Annex 1 for a 'Summary of the Offence'.

2.1 Which organisations are in scope?

The offence applies to **large, incorporated bodies and partnerships** across all sectors of the economy.

2.1.1 What is meant by "incorporated bodies and partnerships"?

Section 199(13) states that the offence applies to organisations incorporated or formed by any means. This includes, but is not limited to incorporation by[5]:

- The Companies Act 2006
- Royal Charter
- Statute (for example NHS Trusts)
- The Limited Liability Partnerships Act 2000
- The Co-operative and Community Benefit Societies Act 2014.

The offence also applies to partnerships which are not bodies corporate (including Scottish partnerships and Limited Partnerships formed under the Limited Partnerships Act 1907).

[5] Note that some charities are incorporated and would therefore be in scope if they meet the criteria to be considered a "large organisation" as described in 2.1.2.

Unincorporated organisations (other than partnerships) are not in scope. **The offence also applies to bodies incorporated and partnerships formed outside the UK but with a UK nexus** (refer to 2.5 on territoriality).

2.1.2 What is meant by "large organisations"?

The offence of failure to prevent fraud applies only to large organisations. A "large organisation" is defined in section 201 as meeting two or three out of the following criteria:

- More than 250 employees
- More than £36 million turnover
- More than £18 million in total assets.

These conditions apply to the financial year of the organisation that precedes the year of the base fraud offence[6].

These criteria apply to the whole organisation, including subsidiaries, regardless of where the organisation is headquartered or where its subsidiaries are located (refer to 2.5 on territoriality). The definition of subsidiaries is given in the Companies Act 2006 section 1159. The provisions relating to subsidiaries are a specific statutory extension of the general principle and only apply to groups where there is a parent-subsidiary relationship. For example, LLP networks, supply chain companies and franchises are not included in this calculation.

For clarity, turnover is calculated as follows:

- 'Turnover' means the amount derived from the provision of goods and services falling within the ordinary activities of the commercial organisation or subsidiary undertaking, after deduction of— a. trade discounts; b. value added tax; and c. any other taxes based on the amounts so derived.[7]
- Aggregate turnover is calculated as: a) the turnover of that organisation; and b) the turnover of any of its subsidiary undertakings (including those operating wholly outside the UK).

Given the large range of legal structures for organisations, this guidance cannot provide details on exactly how the criteria apply to each case. Organisations should take professional legal advice to determine whether they fall into the definition of "large organisation" set out in sections 201-202 of the Act.

[6] Section 199(14) provides the meaning of the term "financial year" for UK companies and for other organisations including overseas bodies.

[7] This is the same definition as used in the Home Office Guidance "Transparency in Supply Chains: a Practical Guide", 2021. Refer also to section 201(5) of the Economic Crime and Corporate Transparency Act, which, for UK companies refers to section 474 of the Companies Act 2006 and which, for organisations which are not UK companies has the same meaning (section 201(5)(b)).

In the remainder of this document, we will use the term “relevant organisation” and “relevant body” interchangeably to mean an incorporated body or partnership that meets the criteria to be considered a “large organisation” and is therefore in scope of this offence.

Subsidiaries

An individual subsidiary or franchise that meets the criteria above would be considered as a “relevant organisation” and could be liable for the offence in its own right. Moreover, t**he subsidiary of a large organisation, which is not itself a large organisation, can be prosecuted rather than the parent organisation if an employee of the subsidiary commits a fraud intending to benefit the subsidiary[8], as set out in section 199(2).**

2.2 Types of fraud covered by the offence

The offence of failure to prevent fraud applies to a number of specific fraud offences, which this guidance refers to as ‘base fraud’ offences. These are listed in Schedule 13 of the Economic Crime and Corporate Transparency Act 2023. Aiding, abetting, counselling, or procuring the commission of any of the listed offences would also qualify as a base fraud offence (section 199(6)(b)).

The offence list can be amended through secondary legislation, if required (section 200).

Relevant organisations can be prosecuted if the associated person’s conduct constitutes a base fraud offence, even if the associated person is prosecuted for an alternative offence or is not prosecuted at all. If the associated person has been convicted of the base fraud offence, this can be used as evidence in proceedings against the organisation for failure to prevent fraud. However, if the associated person is not prosecuted, then the prosecution must prove, to a criminal standard, that the associated person did commit the base fraud offence before the organisation can be convicted of failure to prevent fraud.

2.2.1 Offence list for England and Wales

- Fraud offences under section 1 of the Fraud Act 2006[9] including:
  - Fraud by false representation (section 2 Fraud Act 2006)
  - Fraud by failing to disclose information (section 3 Fraud Act 2006)
  - Fraud by abuse of position (section 4 Fraud Act 2006)
- Participation in a fraudulent business (section 9, Fraud Act 2006)
- Obtaining services dishonestly (section 11 Fraud Act 2006)

[8] Section 199(2) of the Economic Crime and Corporate Transparency Act 2023.

[9] Schedule 13 refers to section 1 offences in the Fraud Act 2006. Section 1 of the Fraud Act creates the offence of fraud and includes the three ways of committing it set out in sections 2-4.

- Cheating the public revenue (common law)[10]
- False accounting (section 17 Theft Act 1968)
- False statements by company directors (section 19 Theft Act 1968)
- Fraudulent trading (section 993 Companies Act 2006).

2.2.2 Offence list for Northern Ireland

- Fraud offences under section 1 of the Fraud Act 2006[11] including:
  - Fraud by false representation (section 2 Fraud Act 2006)
  - Fraud by failing to disclose information (section 3 Fraud Act 2006)
  - Fraud by abuse of position (section 4 Fraud Act 2006)
- Participation in a fraudulent business (section 9, Fraud Act 2006)
- Obtaining services dishonestly (section 11 Fraud Act 2006)
- Cheating the public revenue (common law)
- False accounting (section 17 Theft Act Northern Ireland 1969)
- False statements by company directors (Section 18, Theft Act Northern Ireland 1969)
- Fraudulent trading (section 993 Companies Act 2006).

2.2.3 Offence list for Scotland

- Fraudulent trading (section 993 Companies Act 2006).
- Fraud (common law)
- Uttering (common law)
- Embezzlement (common law).

2.3 Who commits the base fraud and in what circumstances?

As set out in section 199(1), the base fraud offence is committed by a "person associated with the relevant body", described further in sections 199(7)-(9).

An employee, an agent or a subsidiary of the relevant body is automatically an "associated person" for the purposes of this offence. A person who provides services for or on behalf of the relevant body is also an associated person while they are providing those services.

The corporate offences can only take place if the person commits a base fraud whilst acting in the capacity of a person associated with the relevant body (for example, an employee acting in the capacity of an employee, or an agent acting in the capacity of an agent). Fraud that takes place outside this capacity, for example in the person's private life, does not give rise to corporate liability.

[10] Discussion of the extent to which this might overlap with the offence of failure to prevent criminal facilitation of tax evasion can be found in **Error! Reference source not found.**.

[11] Schedule 13 refers to section 1 offences in the Fraud Act 2006. Section 1 of the Fraud Act creates the offence of fraud and includes the three ways of committing it set out in sections 2-4.

The term 'agent' is governed by domestic law and typically includes anyone with authority to enter into contracts on behalf of the relevant body in question. The agent will only be an associated person for a relevant body where the agent is acting in their capacity as an agent for that body. For example, an agent who acts on behalf of multiple entities will only be an associated person of Company A whilst acting as agent of Company A, and not for any activities they conduct on behalf of other companies.

The partners of a partnership that is a relevant body are associated persons. However, where partners commit a base fraud offence which can be committed by a partnership, the partnership may also be liable to be prosecuted for the substantive offence in its own right.

The term "providing services" does not include providing goods. It is also important to note that "providing services for or on behalf of the relevant body" does not include providing services **to** the relevant body. Thus, persons providing services **to** an organisation (for example, external lawyers, valuers, accountants or engineers) are not acting "for or on behalf" of the organisation. This means they would not be associated persons for the purposes of the offence.

Section 199(9) states that "Whether or not a particular person performs services for or on behalf of a relevant body is to be determined by reference to all the relevant circumstances and not merely by reference to the nature of the relationship between that person and the body." **This means that an associated person may or may not be under contract to the relevant body**.

Small organisations should be aware that they may be "associated persons" while they provide services for or on behalf of large organisations. In these circumstances, small organisations may be subject to contractual or other requirements imposed by the large organisations in respect of the offence of failure to prevent fraud.

2.3.1 Subsidiaries

A subsidiary undertaking of a large organisation is an associated person for the purposes of this offence (section 199(7)(a)). This means that it is possible for a **parent company** to be prosecuted for failure to prevent fraud where the base fraud offence is committed **corporately**[12] by a subsidiary and **where the beneficiary is the parent organisation, or its clients to whom the subsidiary provides services for or on behalf of the parent organisation**.

In addition, there are two ways in which frauds committed by the employee of a subsidiary may fall in scope of the offence:

[12] This means that a senior manager of the company, or some other person who represents the "directing mind and will" of the company, has committed the offence while acting in that capacity. (The extension of the identification doctrine to include senior managers is in sections 196-198 of the Economic Crime and Corporate Transparency Act.)

a) If an employee of a subsidiary of a large organisation (where that subsidiary is not itself a large organisation) commits a fraud that is intended to benefit the **subsidiary**, the **subsidiary** may be prosecuted (section 199(2)).
b) If the employee of a subsidiary of a parent company that is a large organisation commits a fraud **that is intended to benefit the parent company**, that **parent company** may be prosecuted (section 199(8)).

The parent organisation is not responsible for unrelated activities by subsidiaries (for example, frauds that are not intended to benefit the parent organisation).

2.3.2 Supply Chain

Companies within an organisation's supply chain are not associated persons unless they are providing services for or on behalf of the relevant body. Where they are providing services for or on behalf of the relevant body, they are associated persons, even if they do not contract directly with the relevant organisation (section 199(9)).

Note also comments on reasonable fraud prevention procedures in 2.6.

2.3.3 Franchises

Individual franchise holders (franchisees) are not associated persons in the same way that subsidiaries are since they are connected to the main franchise company (the franchisor) by contract only and are not undertaking business for the parent company. However, if a franchisee provides services for the franchisor, then the franchisee can be an associated person. This means that the franchisor can be prosecuted for the offence of failure to prevent fraud if the franchisee commits fraud corporately while providing services for the franchisor company. However, an associated person of the franchisee would not be an associated person of the franchisor.

Franchises in Academia

The term “franchise” is used in two special contexts in academia:

“Validation” franchises (where a university with degree awarding powers accredits the degrees of a college that does not have such powers, and the students receive degrees from the university).

“Delivery provider” franchises, where a university or other degree awarding body subcontracts the delivery of its programmes to a delivery provider, while retaining control of the content and quality assurance.

These arrangements are different from the franchise arrangements in companies (described above). Academic franchises may be associated persons for the purposes of the offence depending on the details of the contract. Universities or other degree awarding bodies should take legal advice.

2.4 What is meant by “intending to benefit”?

The issue of who is intended to benefit from the underlying fraud is key to determining whether a relevant organisation can be held accountable for the offence of failure to prevent fraud.

An organisation does not need to actually receive any benefit for the offence to apply - since the fraud offence can be complete before any gain is received. It is enough that the organisation was **intended** to be the beneficiary. The same applies if the intention was to benefit the clients to whom the associated person provides services for or on behalf of the relevant organisation.

Intent to benefit the relevant body is to be judged according to the position of the associated person at the time they commit the fraud offence. It would not be relevant, for example, that the relevant body would be required by regulation to reimburse the proceeds of the fraud were it to be discovered, and therefore might not actually benefit from the fraud in the long run.

The intention to benefit the organisation does not have to be the sole or dominant motivation for the fraud. The offence can apply where a fraudster’s primary motivation was to benefit themselves, but where their actions will also benefit the organisation[13]. The

[13] In the event that the benefits of the fraud accrue to both the individual fraudster and the organisation, there is no threshold in the legislation below which the organisation is deemed not to have benefitted from the fraud. However, prosecutors will apply a public interest case before proceeding with prosecution.

same applies if the intention was to benefit the client to whom the associated person provides services for or on behalf of the relevant organisation.

For example, a salesperson who is on a commission may engage in mis-selling to increase their own commission, but in doing so, they also increase the company's sales. Even though this is not the fraudster's primary motivation, the intention to benefit the company can be inferred in this case because the benefit to the salesperson is contingent on the benefit to the company. As a result, the company may be prosecuted for failure to prevent the fraud.

The benefit may be financial or non-financial. For example, a fraud intended to confer an unfair business advantage would be in scope, as this would constitute an indirect benefit. Equally, a fraud that disadvantaged a competitor would be in scope.

The relevant organisation is not liable if it is a victim or intended victim of a fraud that was intended to benefit the organisation's clients[14] (section 199(3)). The term "victim" is not defined in the Act but, in this case, would apply if the loss caused, or intended to be caused, by the fraud would be borne by the organisation, or the fraud was committed with intent to harm the organisation. However, an organisation would not be a "victim" only because it suffered indirect harm as a result of the fraud by an associated person (for instance, because revelation of the fraud damaged the organisation's reputation). For the avoidance of doubt, an organisation cannot claim that the consequences of being charged with the offence of failure to prevent fraud constitute being a victim of the fraud.

2.5 Territoriality

The offence will only apply where the associated person commits a base fraud offence under the law of part of the UK. This requires a UK nexus. By UK nexus, we mean that one of the acts which was part of the underlying fraud took place in the UK, or that that the gain or loss occurred in the UK[15],[16].

If a UK-based employee commits fraud, the employing organisation could be prosecuted, wherever it is based.

---

[14] Strictly, the persons to whom the associated person provides services for or on behalf of the organisation.

[15] Refer to the Criminal Justice Act 1993, sections 1-2 for application to England and Wales, the Criminal Justice (Northern Ireland) Order 1996 for application to Northern Ireland. There is no equivalent legislation for Scotland covering the question of jurisdiction as regards the Scots common law offences of fraud, uttering and embezzlement. When dealing with these offences, a Scottish court would consider jurisdiction on a case by case basis. Renton and Brown, Criminal Procedure, Vol 1, Part 1, paragraphs 1-18 to 1-20.

[16] Note that, if no part of the base fraud took place in the UK, then there is only a UK nexus if actual gain or loss occurs in the UK, not just intended gain or loss.

If an employee or associated person of an overseas-based organisation commits fraud in the UK, or targeting victims in the UK, the organisation could be prosecuted.

The offence will not apply to UK organisations whose overseas employees or subsidiaries commit fraud abroad with no UK nexus. This would be a matter for law enforcement in the country concerned.

2.6 Defence of reasonable fraud prevention procedures

As set out in sections 199(4) and (5), relevant organisations will have a defence if they have reasonable procedures in place to prevent fraud, or if they can demonstrate to the satisfaction of the court that it was not reasonable in all the circumstances to expect the organisation to have any prevention procedures in place.

The question of whether a relevant organisation had reasonable procedures in place to prevent fraud in the context of a particular prosecution is a matter that can only be resolved by the courts, taking into account the particular facts and circumstances of the case. If a case comes to court, the onus will be on the organisation to prove that it had reasonable procedures in place to prevent fraud at the time that the fraud was committed. In accordance with established case law[17], the standard of proof in this case is the balance of probabilities. Departure from the suggested procedures contained within the guidance will not automatically mean that the organisation did not have reasonable fraud prevention procedures in place.

Chapter 3 sets out key considerations for relevant organisations while developing their fraud prevention procedures. The organisation should put in place fraud prevention measures designed with organisation's structure and the territoriality of the offence in mind.

Depending on the organisation's structure, there are steps that can be taken by parent undertakings to prevent fraud by subsidiaries. For example, implementing group level policies or training and ensuring that there is a nominated person responsible for fraud prevention in each subsidiary. For groups based outside the UK, whether it is appropriate to adopt group wide policies could depend on the extent to which the activities of organisations within the group take place in the UK or give rise to a risk of fraud involving victims in the UK.

In assessing whether the organisation had reasonable fraud prevention procedures in place, a court may take into account that the procedures that an organisation can be

[17] See, for example, R v Boyesen [1982], R v Lambert [2001] UKHL 37, R v Sheldrake [2003] EWHC Crim 273 (Admin)

expected to put in place may be different for employees and agents overseas. For instance, local laws may prevent an organisation from applying the same procedures overseas as it has in place within the UK.

The reasonableness of procedures should take account of the level of control, proximity and supervision the organisation is able to exercise over a particular person acting on its behalf. Where a supply chain involves several entities or a project is to be performed by a prime contractor with a series of subcontractors, an organisation is likely only to exercise control over its relationship with its contractual counterparty.

Where the prime contractor sub-contracts to persons or organisations that could be associated persons of the relevant body, the relevant body may decide to employ the types of fraud prevention procedures referred to elsewhere in this guidance (for example. risk-based due diligence (3.4) and the use of relevant fraud prevention terms and conditions (3.3)) in the relationship with its contractual counterparty, and request that counterparty to adopt a similar approach with the next party in the chain.

In some limited circumstances, it may be deemed reasonable not to introduce measures in response to a particular risk. However, it will rarely be considered reasonable not to have even conducted a risk assessment. Any 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.

The risk assessment should be kept under review. The frequency of review is a matter for the relevant organisation. However, if the risk assessment has not been reviewed recently enough, a court may determine that it was not fit for purpose and therefore that “reasonable procedures” were not in place at the time of the fraud.

2.7 Investigations, penalties and sanctions

2.7.1 How will the law be enforced?

There will always be a base fraud offence which has already been identified.

The offence of failure to prevent this fraud can be prosecuted by the Crown Prosecution Service (for England and Wales), the Crown Office and Procurator Fiscal Service (for Scotland), the Public Prosecution Service for Northern Ireland, and the Serious Fraud

Office (for England, Wales and Northern Ireland)[18] ,[19]. The relevant prosecution service will apply the appropriate code[20] to decide which offence reflects the criminality in any given case. Whether against an individual or corporate, evidential sufficiency and public interest tests will be applied.

The application of fraud prevention procedures by organisations is of significant interest to those investigating fraud and is relevant if an organisation wishes to report an incident of fraud to the prosecution authorities – for example to the Serious Fraud Office (SFO) which operates a policy in England and Wales and Northern Ireland of co-operation with organisations that self-refer incidents of fraud[21],[22],[23],[24]. The organisation's willingness to co-operate with an investigation under the Economic Crime and Corporate Transparency Act and to make a full disclosure will also be taken into account in any decision as to whether it is appropriate to commence criminal proceedings and if so, which type of proceedings (for example, a prosecution or a deferred prosecution arrangement[25]).

Where there is a prosecution, it will be a matter for the court to decide whether any fraud prevention procedures in place were reasonable in all the circumstances.

In many cases, organisations in scope of the offence are subject to a range of other legislation. In cases where a base fraud offence also constitutes a breach of regulations, we expect that prosecutorial bodies and regulators will continue to work together to deliver coordinated resolutions, taking public interest considerations into account. In some cases,

[18] The Serious Fraud Office has investigative powers that extend to Scotland, but prosecution powers in Scotland lie with the Crown Office and Procurator Fiscal Service.

[19] Government is currently conducting a review into private prosecutions. The current situation is that individuals, civil groups or other bodies may prosecute privately in England and Wales.

[20] The Code for Crown Prosecutors in England and Wales, the Prosecution Code in Scotland and the Code for Prosecutors in Northern Ireland.

[21] https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/guidance-for-corporates/corporate-co-operation-guidance/

[22] In Scotland, the Crown Office and Procurator Fiscal Service operates a corporate self-report initiative for instances of bribery under the Bribery Act 2010 and provides guidance on its website: Reporting by businesses of bribery offences: guidance | COPFS.

[23] The Public Prosecution Service in Northern Ireland may take full co-operation into account in applying the public interest test, the second limb of the test for prosecution under the PPS Code for Prosecutors: The Code for Prosecutors | Public Prosecution Service for Northern Ireland (ppsni.gov.uk).

[24] The CPS does not conduct investigations and therefore does not operate a policy of co-operation with organisations that self-refer.

[25] Section 206(3) of the Economic Crime and Corporate Transparency Act 2023 adds the offence of failure to prevent fraud to Schedule 17 of the Crime and Courts Act 2013, which means that deferred prosecutions are available for this offence in England and Wales. **Deferred prosecutions arrangements are not available in Scotland or Northern Ireland**.

regulators could choose to prosecute the offence of failure to prevent fraud themselves, either under any specific powers, or privately[26].

2.7.2 Penalties and sanctions

Section 199(12) sets out the sanctions. If convicted on indictment, an organisation can receive a fine. As set out in sentencing guidelines[27], courts will take account of all the circumstances in deciding the appropriate level of fine for a particular case.

If convicted on summary conviction, the organisation will receive a fine. In Scotland and Northern Ireland this fine may not exceed the statutory maximum.

It is also acknowledged that there are particular challenges involved when fining charities, public bodies and other organisations which provide services to the public. Sentencing guidelines require that when setting a fine, the court must have regard to the impact of that fine on the performance of a public or charitable function.

2.8 Examples

The following examples are illustrative only; they cannot replicate the complexity of real cases. **It should be borne in mind that the offence of failure to prevent fraud is one of a number of mechanisms that could be used to hold a relevant organisation to account following a fraud**.

[26] Some regulators, such as the Financial Conduct Authority, have specific prosecution powers in relation to fraud, while others, such as the Pension Regulator, sometimes choose to prosecute fraud offences privately.

[27] Section 125 of the "Sentencing Code and the Sentencing Council's General Guideline: Overarching Principles" for England and Wales, the Scottish Sentencing Council's "Principles and Purposes of Sentencing" guideline for Scotland and "The Sentencing Guidelines for Northern Ireland" in Northern Ireland.

Examples of fraud by abuse of position

The payroll department of company A is supposed to ensure that the company contributes to the employees' pension funds every month. However, the head of the payroll department arranges for some of these payments to be diverted for other projects within the company but continues to record them as payments to the pension fund. The base fraud is fraud by abuse of position (since the head of the payroll department is entrusted with making payments for the employees), and the associated person is the head of the payroll department. The intention is to benefit other projects within the company. Company A could be liable for the offence under section 199(1)(a) unless a court decides that it had reasonable procedures in place to prevent the fraud.

Example of intended benefits not realised

Example 1: A large company is seeking investments. The accounting department deliberately manipulates the accounts to over-state the profits. The intent of the fraud is to benefit the company by making it appear more attractive to investors. The base fraud here is fraud by false accounting and the associated person is the relevant employee (or employees) in the accounts department. The company could be prosecuted under section 199(1)(a) and could be liable for failure to prevent fraud, unless the court determines that it had reasonable procedures in place to prevent such a fraud. **Note that the offence applies even if potential investment is not actually secured – it is enough that the fraud was *intended* to benefit the company.**

Example 2: An investment fund provider promotes investment in a "sustainable" timber company, knowing that, in fact, this company's environmental credentials are fabricated, and that the timber is harvested from protected forest. Investors are deceived into placing funds with the investment fund provider. The base fraud is fraud by fraud by false representation. The intent is to benefit the fund provider. The associated person is the relevant member of staff at the investment fund provider who knowingly used the false information in the investment fund's brochures for clients. The investment fund provider could be liable under section 199(1)(a) unless a court determines that it had reasonable procedures in place to prevent this fraud. **Again, the offence applies even if the investment is not actually secured – it is enough that the fraud was intended to benefit the investment fund provider.**

Example of a UK nexus in a fraud committed by a company located abroad

A UK Government grant scheme subsidises certain heating appliances if they meet specified efficiency standards. In this example, a small UK manufacturer sends its appliances to an accredited overseas laboratory for efficiency tests. The overseas laboratory has no facilities in the UK. Knowing that the applianeces will not be eligible for grants unless tests demonstrate that the efficiency exceeds a certain threshold, the overseas laboratory manager falsifies the data from the tests. As a result of the fraud, the devices are eligible for grants and the UK manufacturer benefits. In this example, the laboratory manager is the associated person and commits fraud by false representation. Because the effect is to cause an unfair fain to an organisation in the UK, this would amound to fraud under domestic law (and the laboratory manager could theoretically be prosecuted in the UK). The international testing company could be liable for failure to prevent fraud under section 199(1)(b) unless a UK court determines that it had reasonable procedures in place to prevent the fraud.

Examples of an indirect benefit

Example 1: A large healthcare company, A, uses a recruitment company B. There are shortages in the sector and it is difficult to find suitably qualified staff with appropriate eligibility to work in the UK. Company B is supposed to conduct right to work checks on candidates, but an employee of Company A colludes with Company B to falsify documents confirming that these checks have been undertaken correctly. As a result, Company B supplies some staff without eligibility to work to Company A. The “associated person” is the employee of Company A and the base fraud offence is fraud by false representation. The intent is to allow company A to fill its vacancies in order to meet its contracts. Company A could be liable for the new offence unless a court decides that it had reasonable procedures in place to prevent the fraud.

Example 2: A company has an environmental permit from the Environment Agency for limited discharges into a river. As a condition of that permit, the company must provide the discharge data to the Environment Agency. The head of the technical department of that company deliberately falsifies the company’s discharge monitoring system. As a result, the company discharges more pollution than it is allowed to under the terms of the environmental permit. The company provides false data to the Environment Agency, with the intention of avoiding the financial penalties that the Environment Agency can impose. The associated person in this case is the head of the technical department and the base fraud is fraud by false representation. The company could be liable for failure to prevent fraud under section 199(1)(a) if a court determines it did not have reasonable procedures in place to prevent the fraud. This is separate to offences under environmental law.

Examples to illustrate who is the associated person

Example 1: Bank C uses Bank D to provide clearing services. In the course of these clearing services, Bank D (**corporately, with the knowledge and involvement of its senior management**) commits a fraud that benefits Bank C's clients. For the purpose of this offence, Bank D is an associated person of bank C. Bank C is the relevant body that could be liable for the the offence under clause 199(1)(b) unless a court decides that it had reasonable procedures in place to prevent the fraud.

Example of aiding and abetting fraud

Company A is seeking bank lending to purchase new equipment. Employee C of Company A encourages one of Company A's clients (Company B) to make a statement about its intention to place a series of orders with Company A if Company A obtains the equipment. Employee C drafts a letter from Company B to the bank and gives it to Company B to sign. In fact, Company B is winding up its operations and will not be making any such orders. Company B has committed fraud by false representation (it has made a statement it knows to be false in order to make a gain for Company A and has exposed the bank to the risk of loss). Employee C has encouraged and assisted Company B to commit the offence. As Employee C has committed the offence with intent to benefit Company A, Company A could be liable for the offence unless a court decides that it had reasonable procedures in place to prevent the fraud.

Chapter 3: Reasonable fraud prevention procedures

The fraud prevention framework put in place by relevant organisations should be informed by the following six principles:

- Top level commitment
- Risk assessment
- Proportionate risk-based prevention procedures
- Due diligence
- Communication (including training)
- Monitoring and review.

These principles are intended to be flexible and outcome-focussed, allowing for the huge variety of circumstances that relevant bodies find themselves in. As set out in more detail below, procedures to prevent fraud should be proportionate to the risk.

Public sector organisations are already required to implement the recommendations of the Public Sector Fraud Authority[28] and the Government Counter Fraud Profession. They are therefore likely to have many of the elements of the fraud prevention framework already in place. **However, where applicable, they should adapt their procedures to take account of the new offence**.

3.1 Top level commitment

Responsibility for the prevention and detection of fraud rests with those charged with the governance of the organisation. The board of directors, partners and senior management[29] of a relevant body should be committed to preventing associated persons from committing fraud. They should foster a culture within the organisation in which fraud is never acceptable and should reject profit based on, or assisted by, fraud.

[28] https://www.gov.uk/government/organisations/public-sector-fraud-authority (counter-fraud function and counter-fraud profession menus). For organisations in the NHS, the NHS Counter-Fraud Authority provides detailed information on the Public Sector Fraud Authority requirements are to be applied across the NHS and wider health group NHS Requirements | Government Functional Standards | NHS Counter Fraud Authority (cfa.nhs.uk).

[29] Refer to the Glossary for definition of “senior manager”. 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 he “Senior Manager” with responsibility for an organisation’s financial crime compliance systems and controls, or if not, should work closely with them.

Senior management have a leadership role in relation to fraud prevention. The level and nature of their involvement will vary depending on the size and structure of the relevant body, but their role is likely to include:

- Communication and endorsement of the organisation's stance on preventing fraud, including mission statements.
- Ensuring that there is clear governance across the organisation in respect of the fraud prevention framework.
- Commitment to training and resourcing.
- Leading by example and fostering an open culture, where staff feel empowered to speak up if they encounter fraudulent practices.

3.1.1 Communication and endorsement of the organisation's stance on preventing fraud

Effective formal statements to demonstrate the commitment by senior managers within the relevant body may include:

- A commitment to reject fraud, even if this results in short term business loss, missed opportunities or delays.
- Articulation of the business benefits of rejecting fraud (reputational, customer and business partner confidence).
- Articulation and endorsement of the relevant body's policies or codes of practice on fraud prevention and its key fraud prevention procedures.
- Naming the key individuals and/or departments involved in the development and implementation of the organisation's fraud prevention procedures.
- Articulation of the consequences for those associated with the relevant body of breaching the policy on fraud. This may include contractual clauses where appropriate.
- Reference to any membership of collective action against fraud. For example, through initiatives undertaken by trade bodies, etc.

The style and method of communication may vary depending on the target audience. For example, communications aimed at the relevant body's contractors may be different from those aimed at employees.

3.1.2 Ensuring that there is a clear governance across the organisation in respect of the fraud prevention framework

Organisations should ensure that there is clear governance in respect of the fraud prevention framework.

In some organisations, it may be appropriate for senior management to be personally involved in the design and implementation of fraud prevention measures. In other cases, senior management may delegate this task to the Head of Ethics and Compliance or a

similar person who is responsible for the organisation's financial crime compliance and prevention.

Best practice is likely to reflect the following elements:

- Designated responsibility for:
  - horizon scanning for new fraud risks
  - approving the assessment of risk
  - developing and implementing fraud detection measures
  - developing, implementing and testing fraud prevention measures
  - ensuring that appropriate management information is collected and shared to enable senior managers to understand the risks and the effectiveness of fraud prevention procedures
  - developing and implementing disciplinary measures relating to the breach of the relevant body's policies
  - whistleblowing
  - investigations if fraud is detected or suspected
  - monitoring and review of the framework.
- Ensuring that the Head of Ethics and Compliance (or similar person) has direct access to the board or CEO as they think necessary, even if their primary or day-to-day reporting line is to another senior leader or a committee.
- Reporting to the board as appropriate.
- Reviewing the fraud prevention framework and its implementation.
- Minuting decisions and actions.
- Maintaining Governance when members of staff move to other positions, leave the organisation or are off work with illness.

3.1.3 Commitment to training and resource

Best practice is likely to include:

- Senior managers commit to allocating a reasonable and proportionate budget specifically for the leadership, staffing and implementation of the fraud prevention plan, including training. This budget could encompass not only personnel costs but also funding for technology that may include third party due diligence, platforms and related due diligence tools.
- Senior managers commit to resourcing the fraud prevention plan over the long term.
- Senior managers commit to sustaining anti-fraud practices when key members of staff are on annual leave, or off work with illness, or when they leave the organisation.

3.1.4 Leading by example and fostering an open culture

Early action can prevent fraudulent practices from taking hold. Senior managers have a leadership role in fostering an open culture where staff are encouraged to speak up early if they have any ethical concerns, no matter how minor.

According to an article in the CPA Journal[30], fraudsters often rationalise fraud by a variety of techniques:

- Focus on the bigger mission ("someone needs to do this to save the business").
- Focus on responsibility ("it was a group decision", "it's the auditors' job to catch this", "everyone does it").
- Focus on the consequences of the act ("it is not material", "I am levelling the field").
- Focus on the victim ("fraud is a victimless crime", "it's their duty to exercise proper due diligence").

Senior managers can show leadership by challenging these arguments proactively, pointing out the effects of fraud on the business, other colleagues, the sector and public trust. This position may be codified in the organisation's code of ethics or other ethical policies.

3.2 Risk Assessment

The organisation assesses the nature and extent of its exposure to the risk of employees, agents and other associated persons committing fraud in scope of the offence. The risk assessment is dynamic, documented and kept under regular review.

Relevant organisations may already undertake a range of risk assessments relating to fraud and other economic crime. In this case, organisations may find it most effective to extend their existing risk assessments to include the risk of frauds in scope of this offence[31],[32].

Since the definition of an associated person is wide, organisations may wish to start by identifying typologies of associated persons. For example: agents, contractors providing a particular service for or on behalf of the organisation, or staff in specific sensitive roles. Note also comments on reasonable procedures and supply chain issues in 2.6.

---

[30] Journal of the New York State Society of Certified Public Accountants: https://www.cpajournal.com/2019/04/15/rationalizing-fraud/

[31] For example, under the UK Corporate Governance Code, premium listed companies are expected to carry out a robust assessment of the company's emerging and principal risks. These may include fraud risks but may not include all the fraud risks relevant to the offence of failure to prevent fraud. In this case, it would be appropriate for the company to extend the risk assessment.

[32] Similarly, public sector organisations are required to undertake fraud risk assessments as set out by the Public Sector Fraud Authority: Public Sector Fraud Authority - GOV.UK (www.gov.uk) and these should be extended to include risks of frauds in scope of the offence. At the time of writing, the relevant standard is the "Professional Standards and Guidance for Fraud Risk Assessment in Government". The NHS Counter-Fraud Authority provides more specific information on fraud risk assessment in the NHS: Introduction and overview of the new Government Functional Standard 013 for counter fraud | Government Functional Standard | NHS Counter Fraud Authority (cfa.nhs.uk).

Using these typologies, nominated risk owners in the organisation may then consider a wide range of circumstances under which associated persons could attempt a fraud in scope of the offence[33]. Different associated persons may present different fraud risks. For example, fraud by false representation can be committed by a range of associated persons, while frauds by failure to disclose information, false accounting or abuse of position are more likely to be committed by those in certain roles.

It is not possible to anticipate all potential fraud risks. We suggest that the nominated risk owners develop typologies of risks by considering the three elements of the fraud triangle:

- Opportunity
- Motive
- Rationalisation

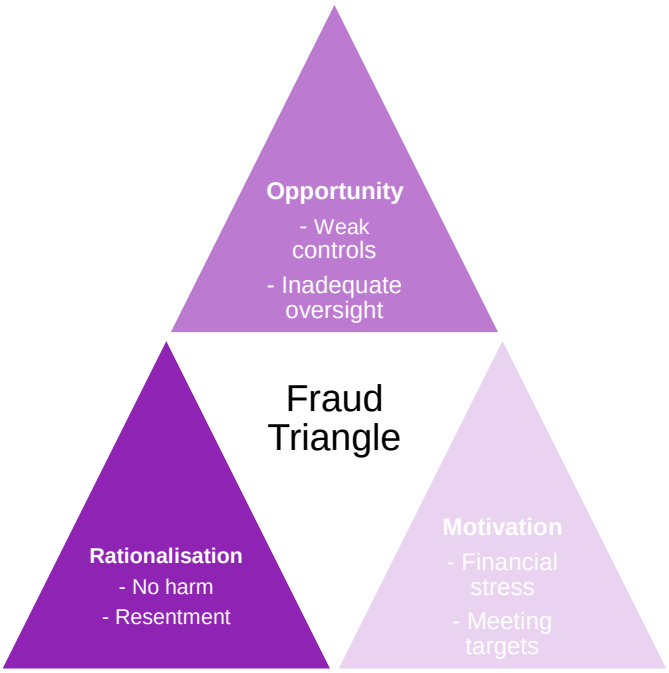

Figure 1: The Fraud Triangle

In developing these typologies, nominated risk owners should take into account the territorial scope described in 2.5.

3.2.1 Opportunity

Nominated risk owners may wish to consider the following questions:

- Do the associated persons have the opportunity to commit fraud?
- Which departments or roles potentially have the greatest opportunity to commit fraud in scope of the offence– for example finance, procurement, investor sales, marketing?

[33] That is, a fraud as set out in Schedule 13 of the Economic Crime and Corporate Transparency Act, or the aiding, abetting, counselling, or procuring the commission. Refer to 2.2-2.5 in this guidance.

- Are there risks associated with taking on agents or contractors who provide services for or on behalf of the organisation? Or are existing contractors and agents exposed to new situations which could increase risk?
- Do some associated persons operate with minimal oversight?
- How likely is detection of any fraud?
- Does churn of staff increase the opportunities for fraud? (For example, cutting corners while the organisation has vacancies in key roles.)
- Do emerging technologies (such as AI) open new opportunities for fraud?
- Could changes in regulation affect the opportunity for fraud?
- Has a previous internal examination or audit highlighted any risk factors for fraud that need to be addressed?
- Have any existing fraud prevention procedures been weakened or neglected?

3.2.2 Motive

Nominated risk owners may wish to consider the following questions:

- Does the reward and recognition system (including commissions or bonuses) incentivise fraud?
- Are there particular financial or operating pressures on the company, for example by way of financial targets/results, an upcoming merger, contract, flotation or other capital raising, loan, permit or licence, grant (e.g. sustainability), or financial reporting dates?
- Do time pressures encourage staff to cut corners, potentially fraudulently?
- Does the corporate culture (including sanctions and penalties) disincentivise whistleblowing when fraud is discovered?

3.2.3 Rationalisation

Nominated risk owners may wish to consider the following questions:

- Is the organisation's culture quietly tolerant of fraud, particularly fraud that might be perceived as securing contracts or jobs for the organisation?
- Is fraud prevalent in this business sector?
- Is it difficult for staff to speak up if they have concerns? Do they face adverse consequences?

3.2.4 Sources of information about potential risks

Sources of information about potential risks include:

- Data analytics
- Previous audits (which may have flagged potential fraud risks)
- Sector specific information, best practice advice or toolkits from relevant professional or trade bodies or regulators[34]
- Regulator enforcement actions (for example, FCA enforcement actions in the financial services sector).

[34] For example, the Food Standards Agency "Food Fraud Resilience Self-Assessment Tool" Food fraud resilience self-assessment tool | Food Standards Agency - although organisations should be aware that some of these fraud risk tools do not cover all the potential frauds covered by the offence.

Over time, there may be prosecutions and/or, in England and Wales, deferred prosecution arrangements (DPAs) related to the offence[35]. Since these are in the public domain, they may be useful for other businesses in the sector when conducting risk assessments.

3.2.5 Emergency Scenarios

Fraud risks may increase during emergencies. By emergencies, we mean events that pose a risk of widespread loss of life or damage to property, or significant financial instability, and that require ameliorating action by the authorities. Failing to undertake any risk assessment for emergencies may mean that the organisation is not considered to have "reasonable fraud prevention measures" in place. For this reason, organisations may choose to include a risk assessment for relevant potential emergency scenarios, while recognising that it is not possible to foresee every emergency.

3.2.6 Classification of risks

The initial risk assessment refers to the "inherent" risks (those risks that exist before any additional fraud prevention measures are put in place). It may be helpful to classify each inherent risk by its likelihood and impact, and to provide a description of why that classification has been chosen. Public sector organisations in scope should follow the relevant risk classification procedures published by the Public Sector Fraud Authority and the Government Counter-Fraud Profession[36] or relevant public sector counter-fraud authority[37].

3.2.7 Review

The risk assessment should be kept under review. The frequency of review is a matter for the relevant organisation, but risk assessments are typically conducted at consistent intervals (annually or bi-annually). Organisations should also consider whether various external factors should trigger an earlier review or a partial review. As part of the review, the risk typologies may be amended as experience is gained and investigations arise.

If the risk assessment has not been reviewed, a court may determine that it was not fit for purpose and therefore that "reasonable procedures" were not in place at the time of the fraud.

---

[35] Section 206(3) of the Economic Crime and Corporate Transparency Act 2023 adds the offence of failure to prevent fraud to Schedule 17 of the Crime and Courts Act 2013, which means that deferred prosecutions are available for this offence in England and Wales. Deferred prosecutions arrangements are not available in Scotland or Northern Ireland.

[36] Government Counter Fraud Profession Standards and Guidance.

[37] For example, the NHS Counter-Fraud Authority

3.3 Proportionate risk-based fraud prevention procedures

An organisation's procedures to prevent fraud by persons associated with it are proportionate to the fraud risks it faces and to the nature, scale and complexity of the organisation's activities. They are also clear, practical, accessible, effectively implemented and enforced.

The relevant body should draw up a fraud prevention plan, with procedures to prevent fraud being proportionate to the risk identified in the risk assessment.

It is a key principle that the fraud prevention plan should be proportionate to the risk and the potential impact. The level of prevention procedures considered to be reasonable should take account of the level of control and supervision the organisation is able to exercise over a particular person acting on its behalf and the relevant body's proximity to that person. For example, a relevant body is likely to have greater control over the conduct of an employee than that of an outsourced worker performing services on its behalf. Nonetheless, appropriate controls should be implemented via the relevant contract.

In some limited circumstances, it may be deemed reasonable not to introduce measures in response to a particular risk. Any 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.

Since the offence extends across organisations in all sectors of the economy, many of these businesses will also be subject to other regulations, for example, regulations concerning financial reporting, environmental, health and safety or competition matters. Processes for compliance with these regulations *may* address certain potential frauds (for example, robust processes for compliance with specific environmental regulations might reasonably be expected to prevent fraud by misrepresentation on the relevant environmental statements).

It is not necessary or desirable for organisations to duplicate existing work. Equally, it would not be a suitable defence to state that because the organisation is regulated its compliance processes under existing regulations would automatically qualify as "reasonable procedures" under the Economic Crime and Corporate Transparency Act.

To avoid duplication of work, organisations are advised to assess whether their existing regulatory compliance mechanisms, financial reporting controls[38] and fraud prevention measures would be sufficient to prevent each of the fraud risks identified in the risk

[38] For example, companies subject to the Financial Reporting Council's "UK Corporate Governance Code" might examine whether their existing controls and procedures under this code would address fraud risks identified in the risk assessment.

assessment (as described in 3.2). Where existing mechanisms appear to be insufficient, organisations should develop appropriate measures to prevent fraud.

Example of examining existing regulatory requirements

The Producer Responsibility Obligations (Packaging Waste) Regulations 2007 (as amended) require regulated companies to meet certain obligations on recycling the waste they produce.

Under these regulations, accredited reprocessors and exporters issue packaging recovery notes and packaging exported recovery notes to represent the tonnage of packaging waste they have recycled, or exported for recycling, to a required standard. These evidence notes are used to offset producers' packaging waste obligations.

In the context of the offence of failure to prevent fraud, we would expect packaging producers, producer compliance schemes, accredited reprocessors and exporters, to examine whether their processes under these regulations are sufficient to prevent fraudulent behaviour (such as issuing or knowingly accepting fraudulent packaging recovery notes or packaging exported recovery notes) and to amend them if not. In the event of a prosecution for failure to prevent fraud, it would not be sufficient simply to state that the company is subject to the Producer Responsibility Obligations (Packaging Waste) Regulations 2007 and therefore it automatically has reasonable procedures in place to prevent fraud relating to these obligations.

When considering the proportionality of reasonable prevention procedures, some suggested risk factors to consider may include the following.

3.3.1 Reducing the opportunities for fraud

- Does the organisation undertake pre-employment and vetting checks? For high-risk roles, does it carry out ongoing vetting checks?
- Do those in high-risk roles receive regular anti-fraud training and how vigorously is compliance with training evaluated or monitored?
- Does the organisation assess emerging risks systematically?
- If new services or associated persons present a potential fraud-risk, is a fraud impact assessment made? What countermeasures can the organisation put in place?
- Are fraud risks managed equally well throughout the procurement process (pre-tender, tender, contract management, during project delivery and project extension)? Do contracts include appropriate terms for associated persons and are these reviewed? Note also comments on reasonable procedures and supply chain issues, in 2.6.
- Does the organisation use best practice with regard to financial reporting, for example, segregation of duties, reconciliation of accounts, suitable sign-off arrangements?

- Have any internal or external audits raised any fraud concerns that have not been acted upon?
- Do procedures for avoiding conflicts of interest need to be bolstered?
- What are the arrangements for limiting access to sensitive or commercial data? Are they kept up to date?
- What is best practice on reducing fraud risks in the sector?[39]

3.3.2 Reducing the motive for fraud

- If there is an existing bonus framework that encourages risk-taking, can any amendments be made to ensure that it does not encourage fraud?
- What can be done to prevent time pressures encouraging staff to cut corners, potentially fraudulently?
- Does the organisation collect information on potential conflicts of interest and keep such information under review?

3.3.3 Putting in place consequences for committing fraud

- What are the internal disciplinary and reporting procedures for those found to be committing fraud?
- Are the outcomes of fraud-related investigations communicated to staff and other associated persons?

3.3.4 Reducing the rationalisation of fraudulent behaviour

Over time, “one-off” frauds may become normalised as people rationalise certain fraudulent behaviours, with arguments such as “other businesses do it”. This phenomenon is known as “ethical fading”. Organisations may wish to encourage proactive challenge of these views as part of their training programmes, and in their organisation’s code of ethics, by pointing out the impact of fraud on colleagues, on the business, on the sector and on public trust. Organisations may also wish to stress that the prevention of fraud is the responsibility of everyone in the organisation, by, for example, incorporating a reminder about the organisation’s code of ethics into performance evaluation.

3.3.5 Sources of information for developing fraud prevention measures

When developing fraud prevention measures, organisations may choose to review relevant sector-specific information. Public sector organisations in scope should follow

[39] For example, local authorities may be members of the National Fraud Initiative, which analyses procurement data and cross references with payroll and Companies House data to support identification of procurement fraud and corruption.

advice on the Public Sector Fraud Authority website[40] or the relevant public sector counter-fraud authority website[41]. Over time, there may be prosecutions or, in England and Wales, DPAs related to the offence[42]. Since these are in the public domain, the anti-fraud measures they contain may be useful for other businesses in the same sector.

Other sources of information, such as Cifas and the Fraud Advisory Panel may be useful.

3.3.6 Emergency scenarios

Public sector organisations in scope should follow specific guidance on fraud prevention in emergency scenarios[43] or relevant information from specific counter-fraud authorities[44].

For private and non-profit sector organisations, good practice includes considering the fraud prevention measures that might need to be taken in emergency scenarios identified in the risk assessment and preparing the transition from emergency measures to business-as-usual measures once the emergency has passed.

It is recognised that not all emergencies are foreseeable and the defence that under the circumstances, it was reasonable not to have any fraud prevention procedures in place *may* apply. One example is when a public authority uses its legal powers to take action to resolve a crisis in the public interest. However, this situation should be time limited. The necessary procedures to prevent fraud should be put in place as quickly as reasonably possible following the crisis and this process should be documented.

3.3.7 Testing the fraud prevention measures

Organisations will want to know how effective their fraud prevention measures are. Best practice is for the prevention plan to be tested by members of the organisation who were not involved in writing it.

---

[40] https://www.gov.uk/government/publications/professional-standards-and-guidance-investigation. At the time of writing, the document is Government Functional Standard Gov S013: Counter Fraud: Management of counter fraud, bribery and corruption activity.

[41] For example, from the NHS Counter-Fraud Authority website.

[42] Section 206(3) of the Economic Crime and Corporate Transparency Act 2023 adds the offence of failure to prevent fraud to Schedule 17 of the Crime and Courts Act 2013, which means that deferred prosecutions are available for this offence.

[43] International Public Sector Fraud Forum guidance - GOV.UK (www.gov.uk). At the time of publication, the document is “Fraud in Emergency Management and Recovery: Principles for Effective Fraud Control”, February 2020.

[44] Such as the NHS Counter-Fraud Authority.

For public sector organisations, guidance on testing fraud controls is provided on the International Public Sector Fraud Forum page of the Government website[45]. These documents may also be helpful for non-Governmental organisations when testing the effectiveness of their fraud prevention measures but there is no expectation that private sector organisations should follow them.

Private sector organisations may decide how to test their fraud prevention measures. However, large organisations that operate internationally may already use various international standards for testing fraud prevention controls[46].
For premium listed companies, there may be some overlap with the UK Corporate Governance Code (which expects the boards of those companies to review and monitor all material controls, including financial, operational and compliance controls, and to report on that review. From 1 January 2026, these companies will also be expected to make a declaration about the effectiveness of these material controls). Where the effectiveness of a specific fraud prevention measure is assessed in the declaration made under the UK Corporate Governance Code, it should not be considered necessary to duplicate the work for the purposes of demonstrating that reasonable procedures were in place to prevent that specific fraud.

Based on the estimated effectiveness of the fraud prevention measures, organisations should qualitatively assess the residual risks.

3.4 Due Diligence

The organisation applies due diligence procedures, taking a proportionate and risk-based approach, in respect of persons who perform or will perform services for or on behalf of the organisation, in order to mitigate identified fraud risks.

Relevant organisations in the sectors facing the greatest fraud risks may already undertake a wide variety of due diligence procedures, both mandatory and in response to risks associated with specific transactions or customers.

However, it should be noted 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. Those with exposure to the greatest risk may choose to clearly articulate their due diligence procedures specifically in relation to the corporate offence.

---

[45] International Public Sector Fraud Forum guidance - GOV.UK (www.gov.uk). At the time of publication, the documents are “The Fraud Control Testing Framework”, September 2023, the “International Public Sector Fraud Forum Guidance”, February 2020 and “Government Functional Standard Gov S013: Counter Fraud: Management of counter fraud, bribery and corruption activity”, Fraud in Emergency Management and Recovery: Principles for Effective Fraud Control”, February 2020.

[46] For example, some international organisations may use the “Evaluation of Corporate Compliance Programs” published by the U.S. Department of Justice.

Relevant organisations should conduct due diligence on associated persons (including new partners). Examples of best practice include:

- Using appropriate technology, for example, third-party risk management tools, screening tools, internet searches, checking trading history or professional or regulated status if relevant, or vetting checks if appropriate.
- Reviewing contracts with those providing services, to include appropriate obligations requiring compliance and ability to terminate in the event of a breach where appropriate.
- Reviewing contracts for agents.
- Monitoring of well-being of staff and agents to identify persons who may be more likely to commit fraud because of stress, targets or workload.

Note also comments on reasonable procedures and supply chain issues in 2.6.

Relevant organisations should conduct due diligence in relation to mergers or acquisitions. Examples of best practice include:

- Using third party merger and acquisition tools.
- Assessment of any relevant criminal or regulatory charges.
- Assessment of tax documentation.
- Assessment of the firm's exposure to risk.
- Assessment of the firm's fraud detection and prevention measures (bearing in mind that if the firm being acquired does not qualify as a "large organisation" as set out in section 201, it may not have any procedures that *directly* address the offence of failure to prevent fraud).
- Integration of fraud prevention measures post-acquisition.

Relevant organisations may choose to conduct their due diligence internally, or externally, for example by consultants. The due diligence procedures put in place should be proportionate to the identified risk and kept under review as necessary.

3.5 Communication

The organisation seeks to ensure that its prevention policies and procedures are communicated, embedded and understood throughout the organisation, through internal and external communication. Training and maintaining training are key.

A clear articulation and endorsement of an organisation's policy against fraud deters those providing services for or on behalf of the relevant body from engaging in such activities. Communication should be from all levels within an organisation. It is not enough for the senior management to say that staff should not commit fraud, if middle management then actively ignore this and encourage junior members to circumvent the relevant body's fraud prevention procedures.

It is important that the relevant body ensures awareness and understanding of its policies amongst those who provide services for or on its behalf. The organisation may feel that it

is necessary to require its representatives to undertake fraud-specific training, depending on the risks it is exposed to. This would be to ensure that they have the skills needed to identify when they and those around them might be at risk of engaging in an illegal act and what whistle-blowing procedures should be followed if this occurs.

It may be helpful to integrate fraud messaging into existing policies and procedures. For instance, policies related to sales targets or customer interactions could include a brief statement addressing fraud rationalisation and the potential consequences of committing fraud.

Organisations may also choose to publicise within the organisation the outcome of investigations, particularly the sanctions imposed.

3.5.1 Training

Training should be proportionate to the risk faced. Consideration should be given to the specific training needs of those in the highest risk posts. Training should cover the nature of the offence as well as the procedures to address it.

Some relevant bodies may wish to incorporate training into their existing financial crime prevention training, while other organisations may wish to introduce bespoke training to address specific fraud risks. Relevant bodies may choose either to train third party associated persons or encourage them to ensure their own arrangements are in place.

Training should include ensuring that staff and other associated persons are familiar with whistleblowing policies. Since whistleblowing is something that staff or other associated persons are likely to do infrequently, it may be helpful to have reminders of the procedures in internal communications.
It is good practice to monitor the effectiveness of training programmes and to ensure that they are kept up to date, particularly as staff move.

3.5.2 Whistleblowing

Transparency International states that “whistleblowing is one of the most effective ways to uncover corruption, fraud, mismanagement and other wrongdoing”[47] . To help prevent fraud, organisations should have appropriate whistleblowing arrangements.

Large organisations may already have whistleblowing processes in place. In some cases, this is a regulatory requirement (for example, the Financial Conduct Authority handbook sets out the expected whistle-blowing procedures for FCA-regulated organisations[48]).

[47] https://www.transparency.org/en/blog/internal-whistleblowing-systems-game-changer and https://www.transparency.org/en/projects/whistleblowing-project

[48] https://www.handbook.fca.org.uk/

Where whistleblowing procedures are required by regulators, organisations should assess whether these procedures would be suitable for the risks identified in the risk assessment.

In cases where organisations are not required by regulators to have whistleblowing processes in place for fraud, or where the existing procedures do not appear to be suitable for the risks identified in the risk assessment, organisations may wish to consider measures such as:

- Having board level accountability to oversee whistleblowing.
- Overseeing a culture where employees feel able to raise concerns.
- Consulting trade unions and/or employee representatives about the content of formal systems for receiving concerns raised by whistleblowers.
- Ensuring that reporting channels for whistleblowers are independent.
- Signposting internal and external whistleblowing arrangements, such as those of the relevant regulators[49] and, if appropriate, trade unions.
- Training staff to ensure that they are aware of how to access whistleblowing arrangements and managers on how to respond when whistleblowing concerns are raised.
- Investigating and responding to internal concerns appropriately and in a timely manner.
- Conducting victimisation risk assessments and protecting whistleblowers from potential victimisation.
- Providing feedback to whistleblowers.
- Learning from the issues raised by whistleblowers.
- Keeping systems under review, including, if appropriate, external assessment of arrangements.

Further information can be found in the Whistleblowing Guidance for Employers and Code of Practice[50]. The charity Protect provides a free confidential helpline for whistleblowers and support to organisations in developing their whistleblowing procedures.

3.6 Monitoring and Review

The organisation monitors and reviews its fraud detection and prevention procedures and makes improvements where necessary. This includes learning from investigations and whistleblowing incidents and reviewing information from its own sector.

3.6.1 Monitoring

Monitoring includes three elements: detection of fraud and attempted fraud, investigations and monitoring the effectiveness of fraud prevention measures.

[49] Whistleblowing: list of prescribed people and bodies - GOV.UK (www.gov.uk)

[50] UK Government publication : "Whistleblowing Guidance for Employers and Code of Practice" https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415175/bis-15-200-whistleblowing-guidance-for-employers-and-code-of-practice.pdf

3.6.1.1 Detection of attempted fraud

Organisations have an interest in ensuring that they are using a range of measures to detect fraud and attempts at fraud. Relevant organisations are likely to have measures in place for detecting frauds against the organisation but may need to consider how these can be extended to frauds that might be intended to benefit the organisation or its clients. Relevant organisations may wish to consider the following questions:

- What analysis is carried out (for example on procurement/payments/invoicing)? How quickly are discrepancies flagged and to whom?
- What processes are in place for detecting unauthorised access to data?
- What data analytics tools are used? Is there scope for use of AI to identify potential frauds?
- What encouragement is there for staff to speak up about fraud-related concerns? Speaking up early prevents small ethical problems snowballing into criminality.
- What are the organisation's whistleblowing procedures? Are they clearly communicated to staff and other associated persons? What action is taken after whistleblowing? Are staff or other associated persons signposted to external whistleblowing sites?
- Is there a nominated member of staff with responsibility for collating and verifying management information on suspected fraud and flagging to the board?

3.6.1.2 Investigation of suspected fraud

Relevant organisations are likely to have in place arrangements for investigating attempted frauds against the organisation but may need to extend them to cover frauds that are intended to benefit the organisation or its clients. Relevant organisations may wish to consider the following questions:

- What factors would trigger an investigation?
- Who authorises the investigations? Are decisions to investigate documented?
- What factors determine whether the investigation is internal or whether an external investigator is appointed?
- What arrangements are in place to ensure that internal investigations are independent?
- What are the arrangements for reporting the results of investigations to the board?
- How are the results of any investigations communicated through the organisation?
- What arrangements are in place for learning from investigations?

Investigations should be independent, clear about their internal client and purpose, appropriately resourced, empowered and scoped (including through legal advice), and legally compliant. Investigations should strive to be fair to all parties. Useful sources of information include the Global Practitioners' Guide to Investigations[51].

[51] Global Investigations Review: "The Practitioner's Guide to Global Investigations", https://globalinvestigationsreview.com/guide/the-practitioners-guide-global-investigations/2021

3.6.1.3 Monitoring of fraud prevention measures

Monitoring fraud prevention measures might include:

- Monitoring of financial controls.
- Collecting data on how many staff have attended fraud prevention training courses and any test results, if applicable.
- Monitoring updates to procedures (for example, due diligence procedures).
- Monitoring updates to contractual clauses for associated persons.

3.6.2 Review

The nature of the risks faced by an organisation will change and evolve over time. This may be as a natural result of external developments, the failure to prevent a fraud by an associated person, or as a result of changes in the organisation's activities. The organisation will therefore need to adapt its fraud detection and prevention procedures in response to the changes in the risks that it faces. The frequency of review is a matter for the relevant organisation, but risk assessments are typically conducted at consistent intervals (annually or bi-annually). Relevant organisations should also consider whether various external factors should trigger an earlier review or a partial review.

An organisation may wish to have its review conducted by an external party or may choose to conduct its review internally.

Relevant organisations can review their fraud detection and prevention procedures by:

- Seeking internal feedback from staff members.
- Reviewing fraud detection analysis.
- Examining any investigations or relevant whistleblowing cases and the subsequent action taken.
- Examining other financial crime prevention procedures.
- Conducting formalised periodic review with documented findings.
- Working with other organisations, such as trade bodies or other organisations facing similar risks.
- Following advice from professional organisations (for example, accountancy or legal bodies).
- Examining any relevant prosecutions or deferred prosecution agreements.
- Collating and verifying management information on the effectiveness of the fraud prevention measures and flagging to the board.

This is not an exhaustive list, and it is expected that organisations will choose the approach most suited to their needs. Relevant organisations may change their review process in light of developments. For example, an organisation may need to take a more formalised and detailed approach to reviewing its fraud detection and prevention procedures following criminal activity by persons associated with it.

As mentioned, relevant organisations may put specific procedures in place during emergency scenarios. Once business as normal has resumed, the organisation should review the effectiveness of the fraud prevention measures during the emergency period.

Chapter 4: Interaction and overlaps between legislative and regulatory regimes

As discussed in chapter 3, there may be overlaps with existing legislative and regulatory regimes. This chapter provides a few illustrations.

4.1 Overlap with the offence of failure to prevent facilitation of tax evasion in the UK and overseas

As set out in Schedule 13 of the Act and **Error! Reference source not found.** of this guidance, one of the base fraud offences included in the scope of the failure to prevent fraud offence is the common law offence of “cheating the public revenue”.

Cheating the public revenue is also one of the base offences caught by the offence of failure to prevent facilitation of tax evasion in the Criminal Finances Act 2017[52].

Cheating can include any form of fraudulent conduct that diverts money from the public revenue or deprives the revenue of money to which it is entitled. Fraudulent conduct means deliberate conduct by the defendant to prejudice, or take the risk of prejudicing, the revenue's right to the tax. It can include both dishonest acts and dishonest omissions to act as required. The offence of cheating the public revenue covers all public revenue including all taxes and duties levied by HMRC. This includes income tax, VAT, duties, loans and grants.

Whilst the base offence of cheating the public revenue and elements therein remain the same for both failure to prevent offences, the overlap is limited to that extent only.

The offence of failure to prevent facilitation of tax evasion is designed to prevent a person associated with a relevant body from criminally facilitating the evasion of tax, and this will be the case whether the tax evaded is owed in the UK or in a foreign country. It should be noted that this offence applies to relevant bodies of all sizes.

[52] The Criminal Finances Act 2017: Criminal Finances Act 2017 (legislation.gov.uk). Guidance on the corporate criminal offence of failure to prevent the criminal facilitation of tax evasion: Corporate offences for failing to prevent criminal facilitation of tax evasion - GOV.UK (www.gov.uk).

The offence of failure to prevent fraud (in this context) is about failing to prevent an associated person from committing the offence of cheating the public revenue[53] with the intent to benefit the relevant body or its clients.

The offence of failure to prevent fraud covers a wider scope in terms of who can commit the offence of cheating the public revenue. Therefore, relevant organisations should be aware that the procedures that they have put in place to prevent the criminal facilitation of tax evasion may not be sufficient, on their own, to qualify as reasonable procedures for the offence of failure to prevent fraud. Relevant organisations should review their procedures and ensure that reasonable preventative measures are in place both in the UK and overseas to specifically address the risks that their organisation could be a beneficiary, or intended beneficiary, of cheats of the public revenue committed by any associated person.

In cases where an organisation could be liable to be charged for both offences, it would be for prosecutors to determine whether the organisation should be prosecuted for failure to prevent facilitation of tax evasion, failure to prevent fraud, or both if the evidential test has been met and if it is in the public interest to do so.
S

4.2 Interaction with auditing requirements

Section 475 of the Companies Act 2006 requires companies to be audited unless they are exempt under sections 477-479 or 480-481[54]. Companies that fall within scope of the offence of failure to prevent fraud are not exempt and are generally therefore required to have an audit[55].

In 2021, the Financial Reporting Council updated its UK auditing standard on the responsibilities of auditors relating to fraud (ISA (UK) 240)[56]. As part of an audit, it is the auditor's responsibility to identify and assess the risk of material misstatement (due to error or fraud) in the organisation's financial statements.

Audits are not required nor designed to identify all frauds and providing a 'reasonable procedures' defence is not the purpose (or a by-product) of an audit. It follows that an audit alone cannot constitute sufficient defence against an accusation of failure to prevent fraud. **Management and those charged with governance should therefore not rely solely on**

[53] Meaning the public revenue in the UK.

[54] This link indicates which UK companies may be exempt and which companies must have an audit regardless of size: Audit exemption for private limited companies - GOV.UK (www.gov.uk)

[55] There may be entities that are exempt from having an audit that still fall within the scope of the offence, for example due to having a qualifying parent (as described in 2.1) or, for companies based overseas, by meeting local (non-UK) requirements.

[56] ISA (UK) 240 (Revised May 2021) - The Auditor's responsibilities Relating to Fraud in an Audit of Financial Statements ISA (UK) 240_Revised May 2021 (frc.org.uk)

the audit to provide them with assurance about the appropriateness of their fraud prevention and detection controls in the context of failure to prevent fraud.

Nonetheless, the auditing process may be useful to the organisation in identifying certain potential fraud risks. For example, auditors hold discussions concerning relevant fraud-related risks with managers[57].

Since some public sector organisations (such as NHS trusts or incorporated local authorities) are in scope of the offence, these organisations may find it helpful to consult relevant papers by the National Audit Office[58].

4.3 Interaction with the UK Corporate Governance Code

Under the UK Corporate Governance Code, boards of premium listed companies are expected to carry out a robust assessment of the company's emerging and principal risks and to report on that work. It also expects these companies to review and monitor all material controls (including financial, operational and compliance controls). The 2024 revisions to the Code will specify that these companies should state whether those controls that the board have agreed are material have been effective as at the balance sheet date. This revision is effective for reporting years beginning on or after 1 January 2026.

Where the principal risks and controls reported on under the Code concern fraud risks identified in the risk assessment for the offence of failure to prevent fraud, there is no need to duplicate that work. However, in practice, they may not cover all the fraud prevention measures that should be considered for the purposes of the offence. In short, compliance with the Code may contribute to an organisation's defence of "reasonable procedures" in the context of the offence, but is not sufficient, on its own, to constitute that defence.

[57] ISA (UK) 240, paragraph 22-1, requires the auditor to discuss with those charged with governance the risks of fraud in the entity, including those that are specific to the entity's business sector and paragraph 43, requires: "The auditor shall communicate, unless prohibited by law or regulation, with those charged with governance any other matters related to fraud that are, in the auditor's judgment, relevant to their responsibilities. In doing so, the auditor shall consider the matters, if any, to communicate regarding management's process for identifying and responding to the risks of fraud in the entity and the auditor's assessment of the risks of material misstatement due to fraud."

[58] For example: NAO report "Tackling fraud and corruption against government", March 2023: Tackling fraud and corruption against government - National Audit Office (NAO) report

Chapter 5: Glossary

‘The Act’ means the Economic Crime and Corporate Transparency Act 2023.

‘Agent’: the term ‘agent’ is governed by domestic law and typically includes anyone with authority to enter into contracts on behalf of the entity.

‘Associated person’ or an **‘associate’** (section 199(7)) means a person who is an employee or an agent of the relevant body, or a person who otherwise performs services for or on behalf of the body. A subsidiary of the relevant body may also be an associated person, if it acts corporately. However, an individual employee of a subsidiary is not an associated person of the parent organisation unless they commit a fraud intending to benefit the parent organisation (section 199(8)).

‘Base fraud' offence means a fraud offence listed in Schedule 13 of the Economic Crime and Corporate Transparency Act 2023 or the aiding, abetting, counselling or procuring the commission of an offence in Schedule 13 of the Act.

‘Incorporated’ means incorporated by any means (section 199(13)), including by:

- The Companies Act 2006
- Royal Charter
- Statute (for example NHS Trusts)
- The Limited Liability Partnerships Act 2000
- The Co-operative and Community Benefit Societies Act 2014
- Organisations incorporated abroad.

‘Large organisation’ means an incorporated body or partnership that meets the criteria in section 201 of the Economic Crime and Corporate Transparency Act 2023.

‘The offence’ means the corporate criminal offence of failure to prevent fraud as set out in the Economic Crime and Corporate Transparency Act 2023.

‘Person to whom the associate provides services for or on behalf of the relevant body’. In a commercial context, this will frequently be a client of the relevant body, however, in a non-commercial context, it may mean any person who receives services, for example, a patient or a tenant (in the case of a local authority). For simplicity, we use the term “client” in this document, regardless of whether there is a commercial contract. The term “client” is not used in the legislation.

‘Relevant body’ means a large organisation that is in scope of the offence under section 199(1). Under the specific circumstances of section 199(2), a relevant body which does not meet the criteria to be considered a large organisation (section 201) can commit the corporate offence, as long as it has a parent undertaking which meets the criteria in

section 202. The term “relevant organisation” is used interchangeably with “relevant body” in the guidance.

‘Residual risks’ means the risks that remain once the measures in the fraud prevention plan are in place.

‘Services’. The term ‘services’ does not include goods.

‘Senior Manager’. Where the guidance refers to liability that arises by virtue of the Economic Crime and Corporate Transparency Act 2023, the definition of senior manager in the Act (section 196(4)) applies. For the purposes of the rest of the guidance, who is a senior manager will depend on context and that while the definition in the Act may be useful, for a regulated body, the meaning applied by regulators may be more appropriate (for example, the definition used in the FCA’s Senior Management Regime).

‘Subsidiary’. The term ‘subsidiary’ is defined in the Companies Act 2006 part 38, section 1159.

Annex 1: Summary of the offence

As set out in sections 199(1)(a) and (b), section 199(2) and section 199(8), the offence of failure to prevent fraud can be committed in a number of different ways. The table below sets out each scenario in terms of who commits the base fraud, who is intended to benefit, and who could be prosecuted for failure to prevent the base fraud.

The offence extends across the UK (refer to 2.2) and under specific circumstances, has extra-jurisdictional reach (refer to 2.5).

<table>
<tr><th>Who commits the base fraud?[59]</th><th>Who is intended to benefit?</th><th>Who could be prosecuted for failure to prevent base fraud?</th><th>Legal reference</th></tr>
<tr><td rowspan="3">An associated person</td><td>The relevant organisation</td><td>The relevant organisation</td><td>199(1)(a)</td></tr>
<tr><td>The clients of the relevant organisation, to whom the associated person provides services for or on behalf of the relevant organisation.</td><td rowspan="2">The relevant organisation, excepy where it is the victim or intended victim of the base fraud (section 199(3)).</td><td>199(1)(b)</td></tr>
<tr><td>The clients of the relevant organisation, where the services to subsidiaries[60] of those clients for or on behalf of the relevant organisation.</td><td>199(1)(b)</td></tr>
<tr><td rowspan="2">The <u>employee</u> of a subsidiary of a large parent organisation.</td><td>The subsidiary</td><td>The subsidiary</td><td>199(2)</td></tr>
<tr><td>The parent organisation</td><td>The parent organisation</td><td>199(8)</td></tr>
</table>

In all cases referring to section 199(1), the base fraud is committed by an “associated person”, for example, an employee of the relevant organisation, an agent, a subsidiary

[59] By “base fraud”, we mean one of the frauds set out in Schedule 13 of the Act, or the aiding, abetting, counselling, or procuring the commission of one of these frauds.

[60] The term subsidiary is defined in the Companies Act 2006 part 38, section 1159. Refer to the Glossary for further details.

(acting corporately) or any other person who provides services for or on behalf of the relevant organisation, regardless of whether the associated person is under contract or not (section 199(9)). The offence only applies when the associated person commits the fraud while acting in their capacity as an associated person or the employee of the subsidiary commits the fraud while acting in their capacity as employee.