FISCAL TECHNOLOGIES

Sapey Associates
Understanding Anti-Fraud Solutions

White Paper

# The Economic Crime and Corporate Transparency Act (ECCTA): Compliance in finance

By Phil Sapey
Sapey Associates
In association with
FISCAL Technologies

# What is the failure to prevent fraud offence?

The Economic Crime and Corporate Transparency Act 2023 is intended to encourage organisations to build a strong anti-fraud culture. It received royal asset on the 26th October 2023, and introduced a new offence: Failure to Prevent Fraud.

The Failure to Prevent Fraud Offence is designed to strengthen the existing powers to fine and prosecute organisations by closing loopholes. Furthermore, although this is a UK law, it applies to organisations outside of the UK if the perpetrator commits the offence in the UK or targets UK victims. This places a responsibility on companies to implement and maintain robust fraud-prevention measures and to demonstrate their effectiveness when required.

According to the UK Government website, 'an organisation will be criminally liable where: a specified fraud offence is committed by an employee, agent or other 'associated person', for the organisation's benefit, and the organisation did not have 'reasonable' fraud prevention procedures in place'. This also applies to subsidiaries or other associated persons who provide services for, or on behalf of the organisation. It's important to note that your organisation doesn't need to be aware of, or order, the fraudulent activity to be liable.

The 'failure to prevent fraud' law applies when an associated person commits fraud that intends to benefit the business. This person could be an employee, intern, volunteer, agent, subsidiary or intermediary - anyone who performs services for, or on behalf of, the organisation.

Please note that an exception would be made if the fraudulent activity was intended to be only for the individual's benefit.

### Offences that fall under this law include:

- Fraud by false representation.
- Fraud by failing to disclose information.
- Fraud by abuse of position.
- Participation in a fraudulent business.
- Obtaining services dishonestly.
- Cheating the public revenue.
- False accounting.
- False statements by company directors.
- Fraudulent trading.

### Examples of this include:

- A public sector organisation awarded a contract to a third-party supplier to deliver services on their behalf due to their low pricing. However, midway through the contract, it was revealed the supplier was able to provide low prices because they were falsifying tax returns (cheating the public revenue). The public sector organisation had not completed due diligence when investigating this supplier. If they had, they would have realised that their pricing model was too good to be true.
- A charity shop manager claims gift aid when they should not. This benefits the organisation to the detriment of HMRC.
- A staff member misrepresents their organisation's green credentials to win a contract. Although the employee does not benefit directly, their organisation does.

Some organisations and departments may be at particular risk of failing to prevent fraud, for example:

- Charity workers might see a deception as being for a just cause.
- A public sector worker might have exacting government targets to meet.
- A member of staff in sales might be trying to hit a performance target.

# Who needs to comply?

The 'Failure to Prevent Fraud' offence applies to large companies. These are 'organisations meeting two out of three of the following conditions in the year preceding the fraud:

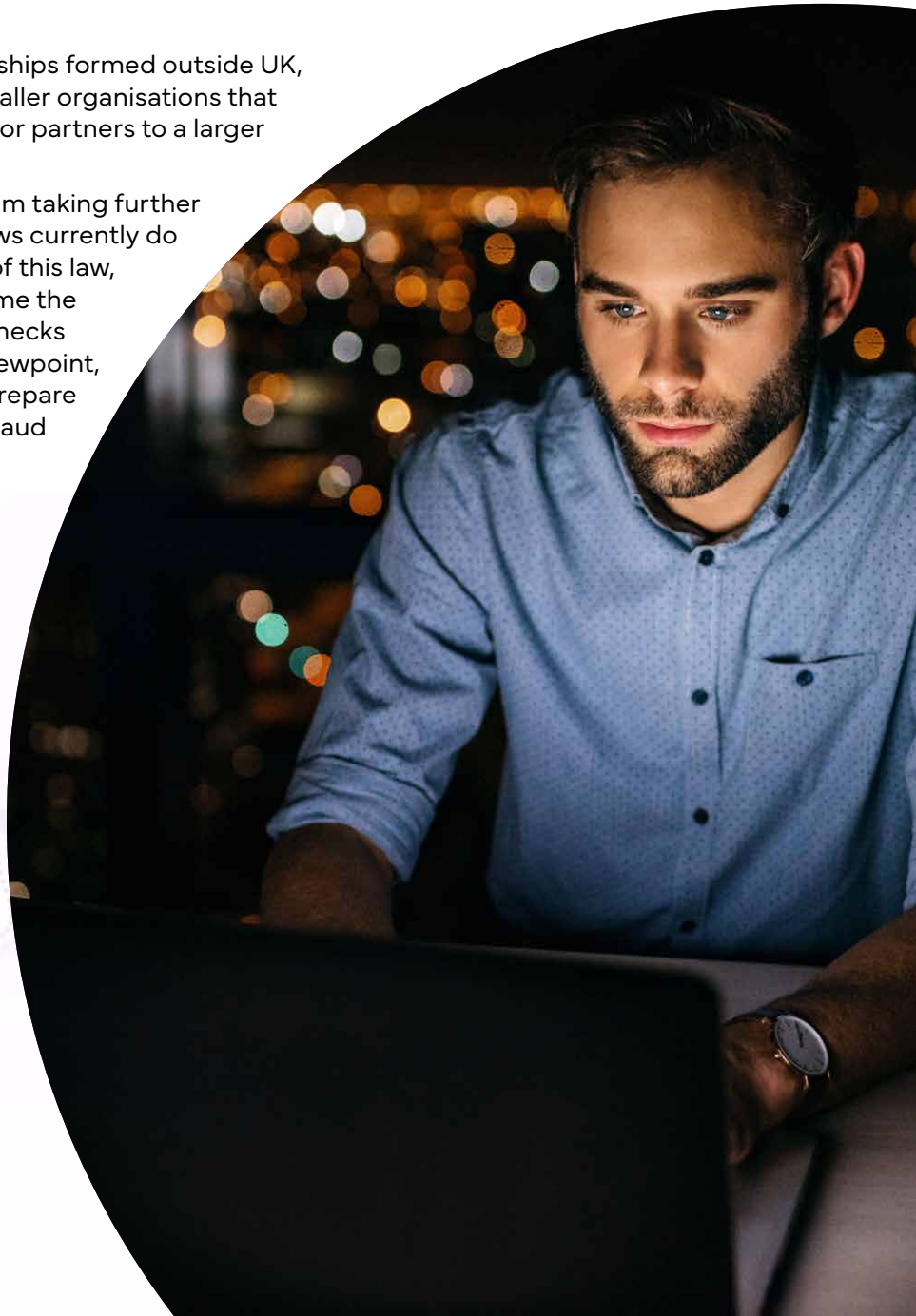
- more than 250 employees.
- more than £36 million turnover.
- more than £18 million in total assets.'

If this is the case for you, then it would be prudent to review your current fraud prevention policies and procedures. Since companies from outside the UK can also be prosecuted, we recommend any company where this applies should take precautions.

## Specifically, the offence applies to:

- All large, incorporated bodies, subsidiaries and partnerships.
- Large not-for-profit organisations such as charities, if they are incorporated.
- Incorporated public bodies.
- Bodies, incorporates and partnerships formed outside UK, with a UK nexus. This includes smaller organisations that could be considered subsidiaries or partners to a larger one.

Other companies can also benefit from taking further preventative measures, even if the laws currently do not apply. It's possible that because of this law, medium-sized companies may become the target of fraud as large companies' checks become more stringent. From that viewpoint, it's a good idea for any company to prepare for this change by having thorough fraud prevention measures in place.



# Guidance on ‘Failure to Prevent Fraud’ offence

The Government has published guidance on this offence, with Nick Ephgrave QPM, Director of Serious Fraud Office (SFO) saying: “The publication of this guidance means that time is running short for corporations to get their house in order or face criminal investigations.”

The guidance was published on 6th November 2024, with a nine-month grace period for affected businesses to review and implement procedures to comply.

## How can you defend against the ‘failure to prevent fraud’ offence?

To comply with the law, organisations must show that: ‘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.’

## What does a reasonable fraud prevention procedure look like?

According to the guidelines set out by the Government, a reasonable fraud prevention framework should be informed by top-level commitment, risk assessment, proportionate prevention procedures, due diligence, communication, monitoring, and review.

To prevent fraud, companies should consider their risks by using the key elements of the fraud triangle: opportunity, motive and rationalisation, create consequences for staff engaged in fraudulent activities, and thoroughly test their fraud prevention measures.


**Overall, companies should complete fraud checks which are appropriate to their risk level.**

## We recommend:

- Articulating a risk appetite and tolerance for fraud, this guides the level of fraud risk a company willing to take at a strategic level and within operational contexts.
- Completing and documenting fraud risk assessments regularly while considering the fraud triangle.
- Develop clear, practical procedures relevant to your fraud risk appetite and organisational complexity.
- Fostering an anti-fraud culture within your organisation by providing awareness and educational programmes for employees and other associates. Embedding a whistleblowing procedure and having a clear process for incident escalation is essential.
- Defining the appropriate level of due diligence for suppliers, employees and other associated persons and conducting these checks thoroughly.
- Decide on the frequency of review required for policies and procedures based on risk appetite, economic climate, market conditions and legislative changes. Consider “fraud-proofing” policies by having them reviewed by a counter fraud specialist or experienced auditor.
- Communicate fraud prevention policies and procedures clearly within the organisation and consider how you will assure the organisation of their effectiveness within the control framework.
- Increase fraud prevention measures during times of increased fraud risk, for example new product launches, organisational restructures and economic uncertainty.

# Undertaking a gap analysis

It is wise for any organisation where the offence applies to undertake a gap analysis. This process helps to identify where existing processes and procedures need strengthening.

You should consider the key elements of the Government's reasonable fraud prevention framework when undertaking a gap analysis. These elements are top-level commitment, risk assessment, proportionate prevention procedures, due diligence, communication, monitoring and review:

## Top-level commitment

In short, top-level commitment means that fraud procedures should begin from the top of the organisation and be backed accordingly by all in management positions.

During your analysis, think on whether you have established clear governance structures to oversee fraud prevention and have allocated sufficient resources for this. Consider if senior management actively promote an anti-fraud culture and the accompanying measures, and if there is regular reporting of fraud prevention activities with clear performance metrics.

Evaluate the robustness of your policies in line with your risk appetite and examine compliance with these policies from the top to the bottom of the hierarchy.

## Risk assessment

In your risk assessment, reflect on how tolerant your organisation is of fraud risk, and whether your operations are within that tolerance. For example, which risks does the organisation consider worth taking? Also ask yourself if you have considered both inherent and residual risks for internal and external fraud in your risk assessment. Another element to consider is how you prioritise fraud prevention activities to ensure the highest risks are always controlled, and how much control you wish to have over risks agreed to be a lower priority. As a final measure for your risk assessments, ensure you regularly update them to reflect any changes in the organisation.

## Proportionate fraud prevention procedure

In terms of proportionality with your level of fraud exposure, you should ensure your anti-fraud policies are consistent with risks identified in the risk assessment, and then assure those controls are effective. This may involve allocating more resource to implement and maintain fraud procedure, and so you need to consider if that resource is currently at an appropriate level. We recommend having a frank discussion with responsible staff members to ensure they have the time and space to do this effectively. You will also need to discuss whether third party relationships are effectively managed and whether there are appropriate procedures in place for that. Think on how effective your staff are at keeping to their fraud prevention procedure, and whether there needs to be further training. If procedure has changed, consider a new training plan to ensure all staff are notified. Lastly, your incident response should be appropriate to your level of risk, and it should also be communicated effectively to all your staff.

## Due diligence checks

Due diligence is an essential part of business, and without it, organisations can quickly become victims of fraud. Consider the checks that are performed when your team screen third parties, whether they are integrated at the right time and level, and whether further checks may be necessary. This is particularly important in areas that are high-risk. These days, it's not enough to screen third parties at an early stage though, they must be monitored continuously. Consider how often checks are carried out and which need to be completed more regularly. Also examine how diligently they are carried out, and whether further training, or regular training, on due diligence procedure may be beneficial. Also ensure due diligence procedures are regularly reviewed and updated, and that there are escalation procedures for any concerns.

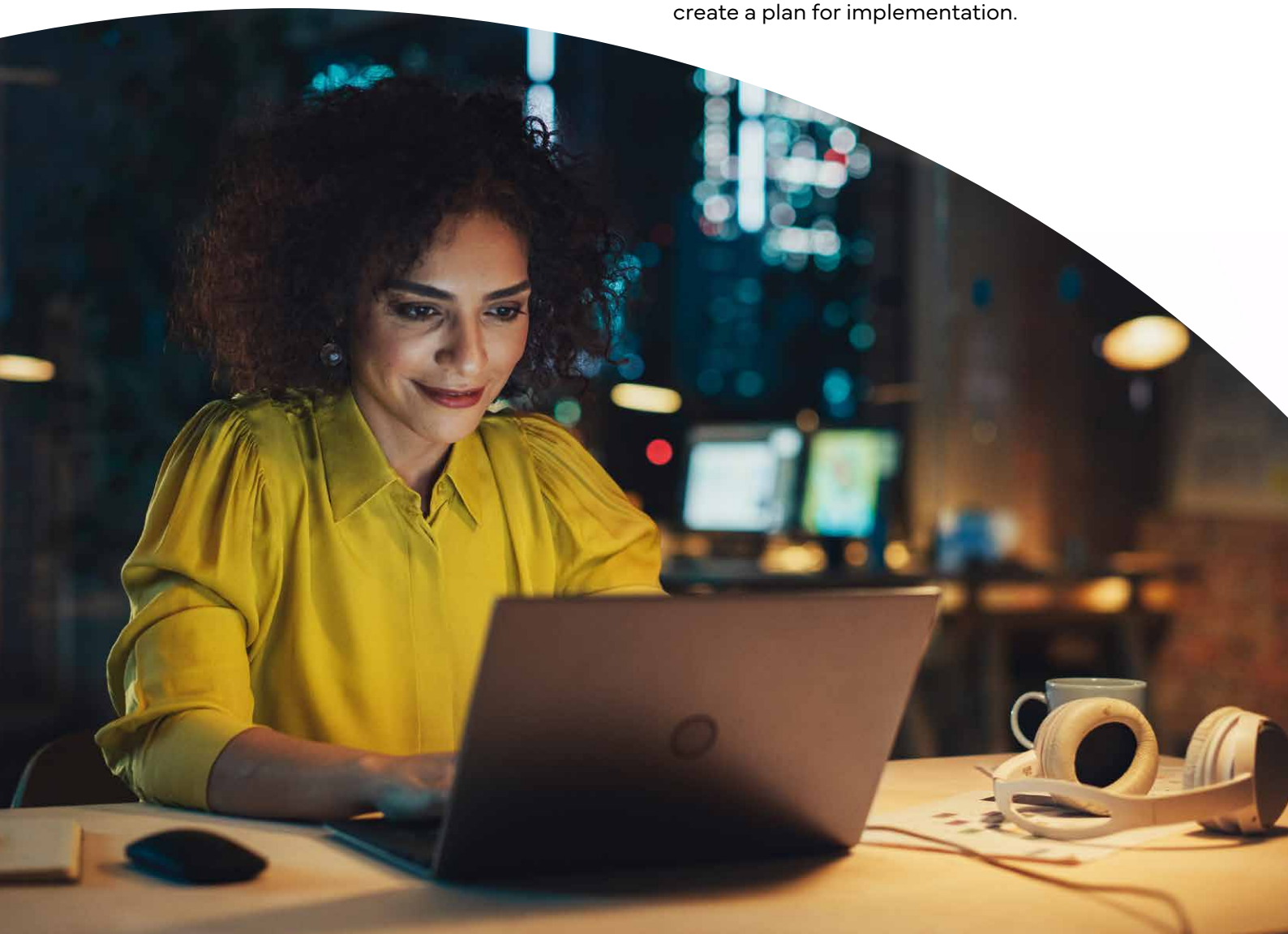
## Communication

Lastly, it's time to review whether your policies are clear and easy to understand for all staff. It should be obvious who is responsible for which actions, and where priorities lie. Your policies should be communicated to everyone in the organisation and should be freely available to view by them. Proper training in all aspects of your procedure should be given, with a training plan in place, for both new and existing members of staff.

## Monitoring and review of risks

Any risk assessment should be reviewed regularly. Consider if there is a plan in place for this, and how regularly they are completed. Measurement of key progress indicators should also be completed regularly, so you can compare how well you are doing, and where areas of the process are falling behind. You should also ensure there is a strategy in place to address any areas falling behind.

In each of these areas, think on the actions necessary to improve your measures and create a plan for implementation.

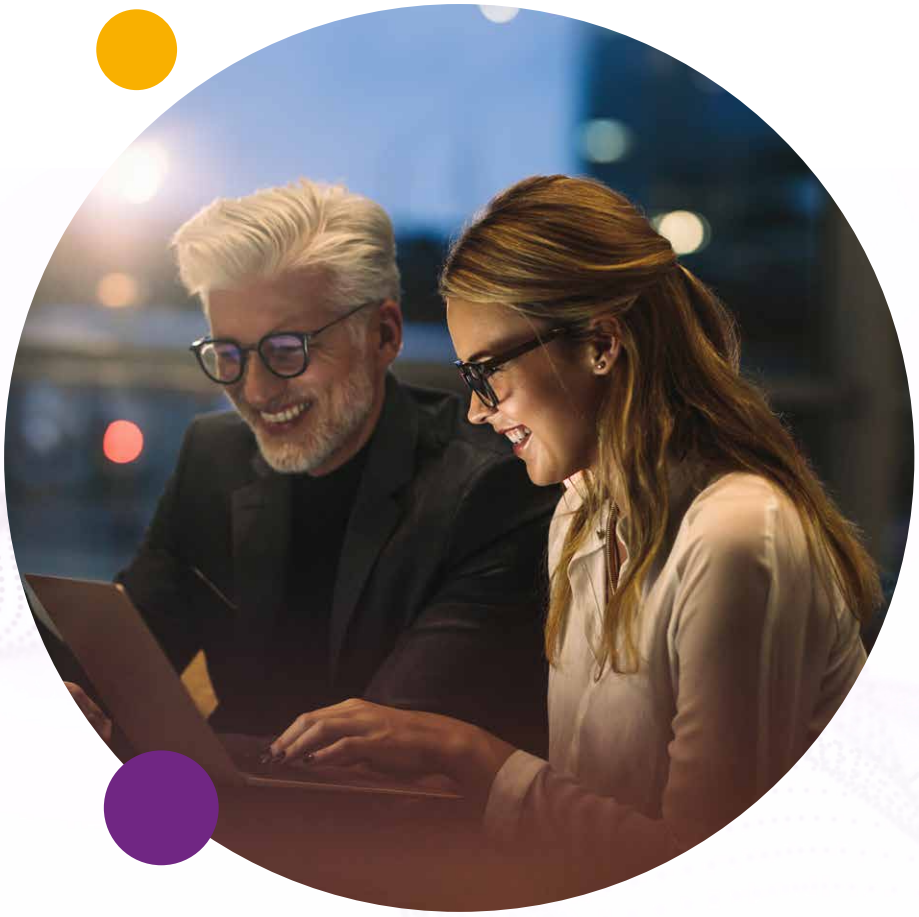


# Further controls for fraud prevention and detection

To create strong anti-fraud measures, we recommend using third party risk management tools. These allow you to undertake various tasks with ease, automating the process to save time and cost:

- Tracking changes in supplier payment information.
- Reviewing your master supplier file often and cleansing it of duplicate, incorrect and dormant suppliers.
- Monitoring inconsistencies in accounts receivable and payable, including balancing suspense accounts.
- Comparing staff information against master supplier files, and alerts when there is an alteration to the master supplier file, including bank account changes.
- Checking purchase card expenses and other expense claims regularly.
- Backing up your records and having a transparent audit trail.
- Making employees and associates aware of your anti-fraud measures as a deterrent.
- Making adverse media, sanctions and credit score checks regularly on suppliers.

We also recommend that your risk detection software is up to date and that your team log in often to check risks.



## How FISCAL helps your organisation check for internal fraud.

Our software solution makes it easy to identify fraud risks and act faster. Using advanced forensics and AI , our platform completes continuous analysis of suppliers and transactions to identify anomalies, which can indicate a fraud risk. Those checks include:

- Employee-to-supplier credential matching.
- Checking the master supplier file for issues including dormant accounts, changes and duplicate suppliers.
- Identifying unusual supplier invoices, such as round amounts, and exceptions or inconsistencies in transactions. This includes Benford's law analysis.
- An audit trail to discover who has made changes, and when.
- Continuous monitoring of suppliers for adverse media, appearance on sanctions lists, and low credit score.

Using FISCAL's fraud prevention software allows you to have greater control around your spend, and who you spend with. It's a high level of oversight, giving you peace of mind.

Sapey Associates
Understanding Anti-Fraud Solutions

## How Sapey Associates understands anti-fraud solutions.

Understanding anti-fraud solutions means being empathetic about the level of controls needed in the context of your organisational environment and having a comprehensive knowledge of fraud prevention frameworks. At Sapey Associates, we can:

- Deliver bespoke fraud and financial crime training based on your specific needs.
- Review the policies and procedures that comprise your fraud prevention framework.
- Assess your organisation's fraud maturity and readiness for the failure to prevent fraud legislation.
- Provide guidance for your investigations.

You can find out more about us and our services at www.sapeyassociates.co.uk

**Disclaimer:**

Please note that this brief should not be treated as a comprehensive explanation of the law, and advice in this document is around sharing best practices based on the Government guidelines. We implore you to seek legal counsel and to consult the Government website for more information on how to comply with this law.

Sources: UK Government website

t: +44 (0) 845 680 1905
e: smarter@fiscaltec.com
w: www.fiscaltec.com



Document ID: Sapey Associates White Paper March 2025