Failure to Prevent Fraud - A Catalyst for Financial Crime Resilience

Fraudulent events in organisations of any size are time-consuming, costly, stressful – even traumatic, and can cause serious reputational damage. And we know that compliance is only the lower rung of the risk ladder - what we should be aiming for is proportionate controls which reflect the actual risk exposures faced. So why not use the heightened awareness brought about by the new Failure to Prevent Fraud Offence, effective from September 2025, to catalyse efforts to build resilience against financial crime in all its guises, mitigate risk, build trust, and protect reputations.

Larger organisations that are in scope for the new Failure to Prevent Fraud Offence, when it comes into force on 01 September, will already be well advanced in their endeavours to comply with this new regime. Under the Economic Crime and Corporate Transparency Act 2023 ('ECTTA'), the threats of criminal liability, unlimited fines, and the reputational harm this may lead to, necessitates this as a priority. But the underlying drivers to this enforced corporate culture shift - ensuring ethical business practices, protecting stakeholders, and fostering integrity to deliver a fairer marketplace, will benefit all stakeholders, and smaller organisations can play their part even if not in legal scope for the offence.

Building Resilience

Fraud prevention efforts to date invariably will have focused on preventing the organisation, its clients, and other stakeholders from falling victim to criminal activity. ECCTA brings in the extra dimension of ensuring that the organisation doesn't itself benefit from fraud conducted by its employees and associates. Consider a professional overbilling clients to inflate his/her own earnings, achieve bonus targets, prestige, or promotion. The employee has committed fraud and can be prosecuted for that, but the organisation also benefits from the extra income and so is liable under the new offence for failing to do enough to stop such behaviour taking place. Whether in scope for the FTPF Offence or not, the organisation's leadership has still failed to implement adequate controls that could have stopped this from happening. Aligned to this line of thinking, Government guidance on the subject stresses that the principles outlined

> "represent good practice and may be helpful for smaller organisations."

The guidance is not dissimilar to other 'failure to prevent' initiatives - Bribery since 2010 and Tax Evasion since 2017, and advocates a framework based on six key principles which if employed effectively, should serve to build resilience and mitigate the risk of prosecution.

1. Leadership and Culture

Leadership at all levels is critical for any cultural change. From the most senior group down to first-level team leaders, all managers need to visibly demonstrate their commitment to embedding a culture aimed at preventing all forms of financial crime. Starting with clear messaging from senior leadership, providing the necessary operational and reporting infrastructure and resources, delivering and participating in awareness sessions, role modelling, and openly recognising exemplary behaviours and positive outcomes - all of these contribute to a culture of integrity and accountability and signify a zero-tolerance approach and commitment to compliance.

2. Risk Assessment

Key is understanding which fraud offences the business could be exposed to, and by whom, not just those specific to ECCTA and the FTPF Offence, but to achieve the widest resilience, all types of fraud and wider financial crime should be considered. This example Financial Crime Prevention Framework provides a checklist of financial crime risks for consideration and can be populated as controls in line with the six principles are developed and implemented for each risk.

Essential to an effective fraud prevention programme is the need for regular and detailed risk assessments to ensure that resources, efforts, and the proportionate procedures required are targeted in the right areas. Such assessments need to consider the organisation's size and structure, sector, products or services provided, markets, jurisdictions and their respective risk levels, supply and distribution networks, and its clients.

Organisations subject to AML (anti-money laundering) regulations will already have resources, risk assessments and proportionate PCPs (policies, controls and procedures) in place for 'know your client' (KYC) compliance demands and source of funds and wealth verification. They might choose to keep this separate or merge it with the wider scope of preventing fraud.

Understanding the 'Fraud Triangle' and how this reflects organisational culture is an important part of assessing the risks. Three elements: incentive; rationalisation; and opportunity, combine to create a culture that can become conducive to fraudulent behaviour:

Understanding these three elements can contribute to an effective risk assessment by unearthing some of the more hidden and cultural elements that might serve to undermine risk controls, for instance:

- Do reward structures pressure people to achieve sales and distribution targets above all else?
- Do client acquisition, retention, or satisfaction targets encourage misselling or misleading statements?
- Is there a low-level tolerance of fraud such as manipulation of purchases, hours worked, or expenses?
- Are discussions about personal behavioural changes left until it is too late because it's 'too difficult'?
- Are there poor controls in place indicating a lack of management that 'deserves to be exploited'?
- Do managers display poor fraud prevention behaviours?
- Are warning indicators ignored, and whistleblowers not taken seriously?

Strategic, operational, and cultural risks can change at any time, so in addition to a regular review, for instance annually as part of a wider risk review, the risk assessment should be considered if there are business model, partnership, market or sector changes, new products or services delivered, or new client groups serviced to assess for any changes in vulnerabilities. Records of each risk assessment should be retained – particularly for those in scope for ECCTA, as this will help support any defence ever needed in respect of decision-making at the time about procedures and resources considered appropriate.

3. Proportionate and risk-based Procedures

Based on the risk assessment findings, a set of controls, proportionate and tailored to the organisation's size, nature, complexity, and specific risk exposures need to be established. Thorough documentation of the outputs of all policies, assessments, and procedures is essential to demonstrate to stakeholders that controls are both implemented and proving to be effective. A set of recommended controls, procedures and evidence is provided in Appendix 1. The proportionality element means that smaller organisations and those with lower risk may have simpler manual controls whilst larger organisations and those exposed to greater risk may need more complex systems and technology solutions.

It is significant that fraud prevention reaches far beyond purely financial controls and personnel, as can be seen by the scope of the procedures and evidence in Appendix 1. The list of operational controls runs from front-end sales and distribution, through to delivery and invoicing and numerous support processes in between including, publicity and media relations, recruitment, and third-party management. Due diligence and performance monitoring of employees, suppliers and agents is to be expected but less expected perhaps is the publicity element.

Public statements made in, for instance, a prospectus, audited accounts and annual statements, or website sustainability and ESG disclosures, all have potential to mislead unless controls are in place to ensure accuracy and can be backed up by hard evidence. The Advertising Standards Agency (ASA) and Competition and Markets Authority (CMA) already have powers to tackle misleading

advertising, with increased powers for the CMA since April 2025 allowing it to directly enforce UK consumer protection laws and issue fines of up to 10% of global turnover, so these could be a source for FTPF prosecutions if they can also be proven to result in fraudulent gains.

4. Due Diligence

Strong due diligence procedures are an important aspect of fraud prevention and are highlighted in the government guidance as an essential part of the risk controls expected to be in place. Due diligence should be applied to scrutinise and verify the integrity of all individuals and businesses associated with and performing services for and on behalf of the organisation. This includes employees and contractors, third party suppliers, advisors, and subcontractors, and agents or other business partners. Depending upon the perceived risk, supply chain integrity may need to be verified at secondary or tertiary levels and even beyond. Scrutiny should be proportionate to the role and fraud risk but is likely to include background checks, financial and credit status reviews, publicity and social media records, and references / testimonials.

Equally, any subsidiaries of an organisation should abide by the same high standards and commitment to prevent fraud, as failure anywhere in the wider enterprise may tarnish the reputation and damage brand value elsewhere. This is reflected in the extra-territorial reach of the FTPF offence as there is potential for prosecution if there is any fraudulent loss or gain for an overseas organisation via a UK connection.

In the regulated sectors, client due diligence is a large part of preventing not only fraud but wider financial and economic crime. Strict 'know your client' regimes need to be applied to serve as gatekeeping to prevent sanctions breaches, money laundering, and bribery and corruption.

Sometimes due diligence might only be applied at the relationship outset and not repeated unless issues arise. Regular due diligence and performance monitoring for both individuals and organisations, defined in employment and business contracts, are straightforward ways to set expectations, conduct regular reviews, and so maintain confidence. In some sectors it is standard practice to complete annual 'fit and proper' declarations and there is opportunity to adapt that approach across a wider field with content tailored to fraud prevention.

5. Communication and Training

Fundamental to achieving the desired objectives of any risk management or change programme is the need to educate everyone within the organisation. This should ensure that awareness and understanding of the fraud prevention policies and procedures are tailored and communicated to all levels and functions in a way which resonates fully with their roles and actual risk exposures. Generic training and over-reliance on eLearning should be avoided. Personalised and in-person delivery allows for discussion in the round to ensure a deeper understanding and adaptation to real-life scenarios. Specifically, tailored training should include how to spot the warning signs of fraud ('red flags'), the controls in place to mitigate risk, and escalation and reporting channels. Training in related areas such as Conflicts, Conduct and Ethics, and Whistleblowing can all play a part in reinforcing integrity overall alongside the education on crime prevention.

With so many other competing risks and information demands, keeping any risk subject on the agenda is difficult. A programme of awareness is needed, including systems for inducting new and returning workers, reminder training for existing workers, and bringing topical issues to everyone's attention. Apart from initial messaging from leaders, subsequent awareness can include stories about investment and resources, proactive efforts, impact success stories (internal and external), and occasional 'war-stories' and lessons learned in the media.

6. Monitoring Review and Improvement

To ensure that fraud prevention measures are both embedded and proving to be effective, organisations should develop a suitable system for monitoring and review. Being transparent about monitoring and metrics used plus the procedures for reporting suspected actual fraud offences, their investigation, disciplinary measures applied, and reporting to external authorities can all serve as effective deterrents. Those controls might include:

- inspections and peer reviews
- forensics / data analytics to identify anomalies
- vigilance, recording, and analysis of red flags
- monitoring of agreed KRIs and KPIs related to fraud and wider financial crime
- incident response plans including reporting, containment, investigation and external reporting where if needed

- speak-up / whistleblowing channels to encourage the reporting of suspicious activities
- independent internal and/or specialist third-party audits
- management review of fraud-related information.

It is important that a continuous improvement mindset is applied to monitoring and review efforts so that the focus is on building and evolving resilience rather than purely on compliance with internal controls and external drivers. Fraud methods evolve rapidly and there is a danger of controls becoming out of date quickly if emerging risks, changes in business operations, and learning from incidents aren't tenaciously acted upon.

People and Culture

People are instinctively biased not to suspect their colleagues of criminal intent and can find themselves making excuses for even the most suspicious behaviours. A starting point is therefore to openly acknowledge that even well-run businesses can fall victim to fraud and that very often, it is a loyal and trusted employee who turns out to be the perpetrator. Raising awareness of this, coupled with monitoring and a supportive culture for speaking out will go a long way to creating an environment where it is hard for criminal activity and any form of misconduct to take hold.

Transparency International considers whistleblowing to be one of the most cost-effective ways to uncover corruption, fraud, mismanagement and other wrongdoing – based on data cited by the Association of Certified Fraud Examiners in its 'Report to the Nations', claiming that 42% of the 2110 cases investigated were detected due to tip-offs. Just as essential to a speak-up culture is a listening one, as a failure to listen and act appropriately can be demotivating and highly damaging to an organisation's reputation. A review of crime prevention controls is a good opportunity to review the internal whistleblowing culture within the business too, considering awareness and comfort levels, anti-retaliation controls, and outcomes. Repeated messaging from the leadership team may be necessary to encourage curiosity and discourage wilful blindness when it comes to fraud indicators.

Despite encouragement, some people still won't speak up for fear of getting their colleagues and/or themselves into trouble. It may then help to reframe speaking up as a way of helping rather than injuring their colleagues who, when it comes to conduct concerns, may be found to be struggling with personal issues that contribute to the incentive element of the fraud triangle. Expensive addictions such as gambling, drugs, or excessive lifestyles can fuel crime to cover spiraling debts, hurting the business and colleagues, as well as family and friends in the process. Some addictions such as gambling are also easily hidden and can be conducted while at work, leading to poor productivity due to distraction and absences for time spent on gambling. Knock-on effects to co-workers are also likely as that lower productivity creates extra work for others who may become resentful, spreading low morale more widely.

In times of uncertainty too, such as in an economic downturn, austerity measures, job cuts, pay freezes, or mergers and acquisitions, organisations need to have a heightened awareness of the impact this may have on individuals, their mental wellness and how this might feed the rationalisation element of the fraud triangle. All endeavours should be applied to manage any uncertainty and provide as much assurance as possible. Astute leaders will have this element in their risk assessment frameworks, and given the current economic landscape, it could be set to medium or high for many organisations.

Further Information

Guidance to organisations on the offence of failure to prevent fraud
2022 ACFE Report to the Nations,
Risk Culture Summary Sheet
Minds in Business Summary Sheet
Appendix 1: Page 5 - Checklist of Policies, Procedures, and Proof

QBE Templates available on the QRisk Client Portal:

Prevention of Financial Crime Framework
Interview & Selection Checklist
Performance and Development Review
Risk Event Review & Improvement Form

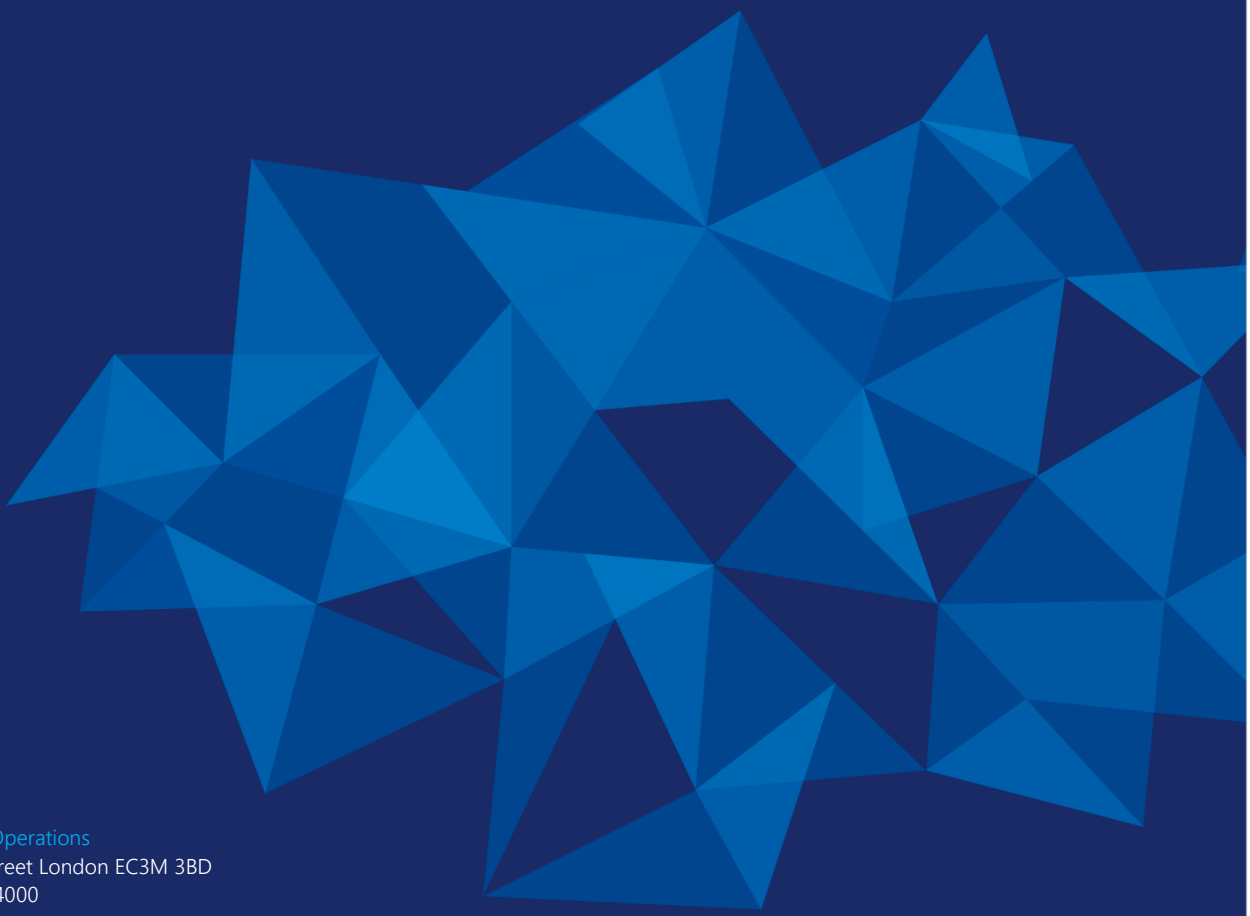
APPENDIX 1 : Checklist of Policies, Procedures, and Proof

The QBE Risk Culture Profiling Tool (self-assessment on QRIsk) can be applied with a crime prevention lens and mirrors closely the six principles advocated for prevent frameworks.

Risk Culture Element	Examples of Procedures (proportionate and risk-based)	Example evidence
Leadership	• Anti-Fraud Policy / Policies (one or several but interconnected and defining scope, appetite, responsibilities, controls, reporting, breach responses) • Leadership promotional statement/s and ongoing encouragement • Regularly reviewed and updated Risk Assessments • Governance oversight • Code of Ethics & Conduct • Advocacy / Lobbying / Sector Initiatives • Annual Review of risk controls, policies, and procedures • Investment in relevant resources, infrastructure, technology	Awareness / Promotional Comms Updates / 'Good news' stories Initial & Subsequent Risk Assessments Board/Senior Management Team (SMT) Agendas & Minutes Agendas and minutes at an management level
Communications	• Authority levels and approval controls for media relations, external statements, social media posts • Commitment and Disclosure statement policy / approval process (e.g. sustainability, ESG, compliance related in a prospectus, annual reports, on websites etc..)	Publications and approvals Fully traceable and auditable evidence linked to statements made in documents / channels
Reward & Recognition	• Staff Remuneration Policy & Criteria (including any bonus plan) • Transparency (part of policy and/or culture) • Partner SLAs, Contracts, and terms of payment	Benchmarking records Call-outs for model behaviour / positive outcomes
People, Training & Development	• Fraud Prevention Champion & Working Group / Committee appointed • Recruitment Policy / Procedures (with due diligence checks) • Regular supervision and annual Performance Monitoring • Training on policies/procedures (tailored to job roles) • Group discussions at team / department level	Role Description/s & Terms of Reference Employee due diligence records Supervision records Performance Reviews Training records & monitoring Team discussion minutes
Operational / Risk Controls	• Sales / distribution procedures (internal / external) • Tenders / bid procedures • (As relevant) Client Due Diligence as part of wider Work/Project and Client Risk Assessments) • Gifts & Hospitality Policy / Procedures • Conflicts Policy • Selection criteria for and appointment of third parties • Purchasing / use of third partes and performance monitoring • Finance and banking controls / procedures • Whistleblowing Policy	Sales plans, targets, and results Tender review and approval records CDD records & approvals Management / Escalation Gifts & Hospitality Records Conflicts reported & resolved Third party due diligence records Contracts to include fraud prevention measures, monitoring & reporting Dual authorisations, suspicious activity investigations / escalations Reports, responses, investigations
Monitoring & Measurement	• Agreed metrics – KPIs / KRIs to be reported including those for governance – can be incorporated into relevant policy or procedure along with red flag indicators • Independent reviews / inspections by peers, supervisors, or automated to include financial angles.	Reports on agreed metrics 'Red Flag' Reviews and outcomes Independent reviews (live and closed projects / work / files)
Continuous Improvement	• Incident response and investigation procedures • Reports / breaches / disclosures reporting procedures • Root cause analyses and action procedures • Independent Internal / External Audit	Containment & Investigation records Disciplinary records Reports / disclosures made Audit reports, recommendations, follow-up & close-out

Deborah O'Riordan
Risk Solutions Practice Leader

deborah.oriordan@qbe.com
+44 020 7105 5528
+44 7786 734 542



QBE European Operations
30 Fenchurch Street London EC3M 3BD
+44 (0)20 7105 4000
qbeeurope.com