Corporate Crime Redefined – The Economic Crime and Corporate Transparency Act 2023

Procurement and Supply Chain Management Made Simple.

Foreword

Corporate criminal responsibility is being redrawn. Economic crime can no longer be understood only through the conduct of a dishonest individual; legislators increasingly examine the surrounding environment – how authority is exercised and whether the organisation tolerated or failed to control the conditions in which wrongdoing occurred. The Home Office estimated the cost of fraud to individuals and businesses in England and Wales at £14.4 billion in the year to March 2024.

For decades, organisations drew a sharp line between personal misconduct and corporate responsibility. A dishonest employee faced investigation while the employer maintained that the conduct was unauthorised and contrary to policy. That distinction has narrowed. Contemporary economic-crime legislation increasingly asks whether wrongdoing was undertaken for organisational benefit, and whether governance arrangements were robust enough to prevent people acting on the organisation's behalf from committing the relevant offences.

The shift reflects modern corporate structures. Large organisations rarely operate through a single decision-maker with complete control; authority is distributed across boards, divisions, subsidiaries, outsourced providers and intermediaries, so commercial activity may be carried out by people considerably removed from central leadership. Corporate responsibility must therefore consider not only who formally directs the organisation, but who performs services on its behalf and how that activity is supervised.

Culture matters because formal rules alone rarely determine behaviour. Employees may receive clear instructions prohibiting dishonesty while facing aggressive sales targets, unrealistic deadlines or pressure to secure results. The Association of Certified Fraud Examiners' 2024 global study estimated that the typical organisation loses around 5% of annual revenue to fraud, a conservative figure given how much fraud goes undetected. Where performance is rewarded regardless of method, dishonesty becomes easier to rationalise.

Controls provide a further layer of accountability. Approval procedures, segregation of duties, due diligence, training and monitoring can all reduce opportunity, but their value depends entirely on implementation. A policy that exists only on paper offers little protection if employees routinely bypass it or if management tolerates repeated exceptions. Effective governance therefore depends less on whether controls exist than on whether they operate consistently and respond proportionately to risk.

External relationships extend the boundary of responsibility further still. Organisations increasingly rely on agents, contractors, consultants and outsourced providers to deliver core activities, and those parties may interact with customers, administer transactions or represent the organisation externally. Fraud risk therefore does not stop at the employment boundary; understanding who acts for an organisation, what authority they hold, and how their conduct is controlled has become a central governance question.

Corporate exposure to economic crime is now a governance issue rather than a disciplinary one. Responsibility extends to culture, incentives, delegated authority, third-party relationships and the effectiveness of preventive controls. The Economic Crime and Corporate Transparency Act 2023 turns that broader question into law: whether the organisation created and maintained an environment capable of preventing fraud committed for its benefit, and whether it can demonstrate reasonable measures were in place before misconduct occurred.

Why Corporate Crime Was So Difficult to Prosecute

For offences requiring proof of dishonesty, knowledge or intention, prosecuting a company traditionally depended on the identification doctrine. The prosecution had to identify an individual whose position and authority made them the company's "directing mind and will"; only then could that person's conduct and state of mind be attributed to the company itself. Without such an individual, the company generally escaped criminal liability, however serious the underlying misconduct.

The doctrine developed through case law and is most closely associated with the House of Lords decision in Tesco Supermarkets Ltd v Nattrass (1972). It reflected the difficulty of applying concepts such as intention or dishonesty to an artificial legal person. Because a company cannot think or act independently, the law sought individuals whose actions could be treated as the company's own, rather than merely those of ordinary employees or agents.

The approach caused fewer problems in small organisations, where authority sat with one or two senior individuals. An owner-director might exercise sufficient control over the whole business to satisfy the test easily. As companies expanded, however, authority became distributed across boards, divisions, subsidiaries and specialist management teams, making it progressively harder to identify any one person who represented the directing mind and will of the organisation as a whole.

Modern corporate structures exposed a widening mismatch between legal theory and commercial reality. A senior executive could hold substantial authority over a business unit, market or transaction and still fall short of the traditional attribution test. Decisions capable of causing serious economic harm might be made by several executives acting within delegated responsibilities, none of whom individually possessed sufficient control to be characterised as the company itself.

The result was that large, complex organisations could be harder to prosecute than small businesses for offences requiring a guilty state of mind. Prosecutors might demonstrate serious misconduct by senior personnel, significant benefit to the company and substantial organisational failings, yet still be unable to establish attribution. Complexity, delegation and fragmented decision-making could therefore become a shield against liability rather than a governance weakness to be addressed.

The 2014 Tesco accounting scandal illustrated the problem starkly. Tesco Stores Limited overstated half-year profits by £326 million, later settling with the Serious Fraud Office through a 2017 deferred prosecution agreement worth £129 million plus £3 million costs. Yet the identification doctrine defeated the individual prosecutions: three former directors were acquitted or discharged between 2018 and 2019, the judge finding the evidence against two of them too weak for a jury to convict.

Criticism of the doctrine, therefore, focused on fairness and accountability, not merely on enforcement difficulties. A test developed for simpler corporate structures appeared increasingly unsuited to multinational groups, financial institutions and organisations in which authority was deliberately dispersed. The Economic Crime and Corporate Transparency Act 2023 first addressed that criticism with a statutory attribution route limited to specified economic crimes; the Crime and Policing Act 2026 then generalised the same model to all criminal offences.

The Economic Crime and Corporate Transparency Act 2023

The Economic Crime and Corporate Transparency Act 2023 (ECCTA) is a substantial development in the UK's response to fraud, money laundering and the misuse of corporate structures. Receiving royal assent on 26 October 2023, it forms the second major part of a legislative package that began with the Economic Crime (Transparency and Enforcement) Act 2022, aiming to make the UK business environment more resistant to economic crime and to improve the reliability of corporate information.

The Act's reforms extend well beyond corporate criminal liability. They include strengthened Companies House powers, greater transparency in company ownership, reforms to limited partnerships, enhanced powers to seize and recover suspected criminal cryptoassets, and measures to support information sharing against money laundering. Companies House, which held around 5.4 million companies on its register in June 2025, is becoming an active gatekeeper with new powers to query, reject, and remove information, thereby improving the register's accuracy.

Within that broader programme, the corporate criminal liability provisions mattered most for organisations, because they addressed longstanding difficulties in holding companies themselves responsible for economic wrongdoing. Section 196 originally reformed the identification principle for specified economic crimes, attributing liability to the organisation whenever a qualifying senior manager committed an offence within their actual or apparent authority. That provision has since been repealed and superseded, as explained below, but it remains the origin of the wider senior-manager model.

The Act also creates a separate failure to prevent fraud offence under section 199, fundamentally changing how qualifying organisations must consider fraud committed by associated persons for the organisation's benefit or, in defined circumstances, for the benefit of clients. Rather than requiring prosecutors to prove that leadership authorised or knew about the fraud, liability turns on the conduct of associated persons and whether reasonable prevention procedures existed.

These reforms form part of a wider shift away from treating economic crime solely as individual misconduct. The Government pledged £63 million to fund Companies House reform between 2022-23 and 2024-25, while its own impact assessment forecast £289 million in compliance costs to business – a cost it judged justified by the value of a more reliable register. For large organisations, the failure-to-prevent regime now places preventative governance at the centre of economic-crime compliance.

Two New Routes to Corporate Criminal Exposure

Corporate criminal exposure for economic wrongdoing now rests on two distinct mechanisms that should not be treated as interchangeable and that, since 29 June 2026, sit in two different Acts. The first concerns attribution: under section 250 of the Crime and Policing Act 2026, any offence committed by a senior manager can be treated as an offence of the organisation itself where the manager acts within the actual or apparent scope of their authority.

The second mechanism, set out in ECCTA sections 199 to 206 and Schedule 13, is the failure-to-prevent-fraud offence, which remains untouched by the 2026 reform. It does not depend on attributing the fraudulent person's state of mind to the organisation through senior management. Instead, a qualifying large organisation may incur liability where an associated person commits a specified fraud intending to benefit the organisation or, in prescribed circumstances, a client, and reasonable fraud-prevention procedures were not in place.

The distinction carries real practical consequences. Section 250 of the Crime and Policing Act 2026 asks whether a senior manager personally committed any offence while acting within their authority, allowing that offence to be attributed to the company, with no equivalent reasonable-procedures defence. Failure to prevent fraud asks a different question entirely: whether fraud by an associated person occurred in circumstances that engage the statutory offence, and whether the organisation can establish the reasonable-procedures defence.

The two routes, therefore, expose organisations to liability for different reasons and through different categories of people. One broadens attribution for any offence committed at senior-manager level; the other imposes a preventative obligation on large organisations regarding fraud by associated persons more generally. Maintaining that distinction matters because the failure-to-prevent regime is not an extension of section 250, and section 250 does not depend on any failure of fraud-prevention controls.

The Senior Manager Test – Expanding Corporate Attribution

Section 196 of ECCTA first attributed specified economic crimes to a body corporate or partnership where a senior manager committed an offence, effective from 26 December 2023. Section 250 of the Crime and Policing Act 2026 has since replaced it, extending the same principle to any criminal offence from 29 June 2026: the prosecution no longer needs to prove a directing mind, only that a senior manager committed the offence within the organisation's actual or apparent scope of authority.

The authority requirement matters because section 250 does not require the organisation to have authorised criminal conduct. The relevant question is whether the senior manager was acting within an activity they were actually or apparently empowered to undertake. A finance director authorised to make statements about financial performance, for example, may engage corporate liability if deliberately false statements amounting to any criminal offence are made within that apparent sphere of responsibility.

Under ECCTA, the mechanism applied only to offences listed in Schedule 12 – a list spanning fraud, false accounting, bribery, money laundering, fraudulent trading and certain tax offences, together with secondary participation in them. Section 250 of the Crime and Policing Act 2026 removed that boundary entirely: the offence list no longer matters, because any criminal offence under the law of England and Wales, Scotland or Northern Ireland can now trigger attribution.

Unlike the failure to prevent fraud offence, section 250 is not confined to organisations meeting the statutory definition of a large organisation. A body corporate or partnership may fall within the attribution provision regardless of turnover, employee numbers or balance-sheet size, provided the statutory conditions are satisfied. This means smaller and medium-sized organisations may face section 250 exposure even though they sit outside the failure-to-prevent regime's principal scope.

Section 250 also operates alongside, rather than abolishing, the common-law identification doctrine. Prosecutors may still rely on traditional attribution principles where appropriate, while the statutory route now provides an additional mechanism for any offence, not merely economic crime. This matters particularly in complex organisations where significant authority is distributed among senior personnel, reducing the need to identify a single individual with sufficient authority to be the organisation's directing mind and will.

The practical effect is to bring corporate exposure closer to how organisations are actually run, and to extend it across the full range of criminal offences rather than economic crime alone. Where senior managers exercise substantial delegated authority over finance, commercial operations, procurement or sales, their offending may have direct consequences for the organisation, even without board membership. Organisations must therefore map where meaningful authority actually sits, since attribution follows practical responsibility rather than the organisation chart.

Who Is a Senior Manager?

The statutory definition of a senior manager is deliberately functional. First set out in section 196 of ECCTA and carried over unchanged into section 250 of the Crime and Policing Act 2026, it focuses on what an individual actually does and the significance of their role, rather than on a job title, grade, or position on an organisational chart. A prestigious title alone will not suffice if the person lacks the necessary managerial influence.

A senior manager is someone who plays a significant role either in deciding how the whole or a substantial part of the organisation's activities are managed or organised, or in actually managing or organising the whole or a substantial part of those activities. The wording captures both strategic decision-making and substantial operational management, recognising that meaningful corporate authority can be exercised through different structures and at different levels.

In practice, the test may capture divisional directors, commercial directors, finance leaders, procurement leaders and other senior operational managers whose responsibilities cover a substantial part of the organisation's activities. Whether a particular individual qualifies depends on the facts: responsibility for a major division, a material revenue stream, or a strategically important function may matter more than whether the individual formally sits on the board or holds an executive title.

The phrase "substantial part" is therefore important. It prevents the test from applying only to those who manage the entire organisation, while still distinguishing senior management from employees whose responsibilities remain comparatively narrow. A person controlling a significant business unit or function may fall within the definition even where other executives hold greater overall authority – assessment turns on organisational significance and decision-making influence, not job title.

For governance purposes, organisations should look beyond formal delegations to identify where senior managerial power actually operates. Responsibility matrices, committee terms of reference, delegated authorities and job descriptions provide evidence, but actual behaviour can matter just as much. A procurement or finance leader who routinely makes decisions beyond a narrowly drafted job description may present a different attribution risk from that suggested by documentation alone.

Failure to Prevent Fraud – The New Corporate Offence

The failure to prevent fraud offence, introduced by section 199 of ECCTA, came into force on 1 September 2025. It marks a significant change in corporate criminal responsibility because liability can arise without proving that directors or senior managers participated in, authorised or even knew about the underlying fraud. The focus instead shifts to fraud committed by associated persons and the adequacy of the organisation's fraud-prevention arrangements.

A qualifying large organisation may commit the offence where an associated person commits one of the specified fraud offences while acting in that capacity, intending to benefit the organisation directly or indirectly. The legislation therefore addresses conduct undertaken to improve revenue, secure contracts, protect financial results or obtain another advantage for the organisation, even where those governing it remained entirely unaware of what occurred.

The offence also applies where the associated person intends to benefit a person to whom, or to whose subsidiary undertaking, services are provided on the organisation's behalf. In commercial settings, this commonly involves a client, though the statutory language is broader than that of a conventional client relationship. It recognises that organisations that deliver services to others through employees, agents, or intermediaries may face fraud intended to benefit those recipients.

An important limitation applies where the organisation itself is the victim or intended victim of the underlying fraud. Section 199(3) is designed primarily to address fraud committed for the organisation's or a client's benefit, not every dishonest act committed against the business. An employee stealing from an employer, for example, presents a materially different legal position from an employee making dishonest representations to secure commercial advantage for that employer.

Where the statutory conditions are established, the organisation has a defence if it proves that it had reasonable procedures in place, at the time of the fraud, to prevent associated persons committing fraud of that kind – or that it was reasonable in all the circumstances not to have such procedures. That defence makes preventative governance, proportionate controls and demonstrable implementation central to the organisation's legal position.

The significance of the offence lies in the separation of corporate liability from senior-level knowledge. An organisation cannot necessarily avoid exposure by showing that fraudulent conduct was concealed from the board or contradicted formal policy. The relevant questions become who committed the fraud, in what capacity, whom it was intended to benefit, and

whether reasonable prevention procedures existed – extending corporate responsibility beyond top-down instructions to the systems operating throughout the business.

Which Organisations Are Caught?

The failure to prevent fraud offence applies only to a "relevant body" that qualifies as a large organisation under sections 201 and 202. Broadly, an organisation is large if, in the financial year preceding the year of the underlying fraud, it satisfies at least two of three conditions: more than 250 employees, turnover exceeding £36 million, and balance-sheet assets exceeding £18 million. The thresholds combine workforce, commercial scale and asset measures.

The regime is not confined to trading companies. Incorporated bodies and partnerships fall within scope, including incorporated charities, certain incorporated public bodies, limited liability partnerships and organisations incorporated outside the UK where the necessary territorial connection exists. Unincorporated bodies other than partnerships generally fall outside the offence, so both legal form and financial scale matter when determining whether an organisation is caught.

Care is required where the organisation is a parent undertaking. Section 202 applies group-based calculations, so turnover, balance-sheet totals and employee numbers are assessed across the parent and its subsidiary undertakings. A parent cannot assess exposure simply by examining its own standalone accounts; group structures may bring entities within the large-organisation regime even where an individual company, viewed alone, falls below the thresholds.

Subsidiary undertakings require careful analysis because the legislation establishes specific routes through which fraud within a corporate group can give rise to liability. Fraud committed by, or within, a subsidiary can expose either the subsidiary itself or a qualifying parent where the statutory benefit conditions are satisfied. Determining scope, therefore, requires organisations to map group relationships and examine where services, authority, and intended benefits actually flow.

Associated Persons – Liability Beyond Employees

The concept of an "associated person" is central to the failure to prevent fraud offence, as it determines whose conduct may expose an organisation to liability. The legislation expressly includes employees, agents and subsidiary undertakings, but is not limited to those categories. A person who otherwise performs services for or on behalf of the organisation may also qualify, thereby extending the analysis well beyond conventional employment to encompass wider commercial arrangements.

For other persons, section 199(9) states that the test is determined by all relevant circumstances, not merely the formal nature of the relationship. A written contract describing a party as an independent contractor, supplier or consultant is not conclusive. The practical question is whether the person was performing services for or on behalf of the relevant body when the underlying fraud was committed in that associated capacity.

The associated-person concept can also extend risk through corporate groups. A subsidiary undertaking may itself commit corporate fraud, while employees of subsidiaries can engage in specific provisions where the intended beneficiary is the subsidiary or a qualifying parent. Organisations therefore need visibility beyond their direct employees and immediate contracting entities, since group functions, shared services, and externally delivered operations can all create relationships that require assessment.

Employees, Agents, Contractors and Intermediaries

Employees are the most obvious associated persons, but their significance extends beyond ordinary employment duties. Fraud risk may arise in sales, procurement, finance, customer service, claims handling or regulatory reporting, wherever an employee can make

representations or manipulate information for organisational benefit. Prevention arrangements should reflect actual responsibilities, commercial pressures and opportunity, rather than relying on generic conduct policies or annual awareness training alone.

Sales agents and distributors can present particular exposure where they promote products, negotiate contracts or otherwise act as the organisation's route to market. Commission structures, ambitious targets and limited supervision may increase the risk of dishonest statements intended to secure business. Whether a distributor is an associated person depends on the services it actually performs for or on behalf of the organisation, not the label used in its contract.

Consultants, outsourced providers and professional advisers require a more nuanced assessment. A professional adviser or firm merely providing advice or specialist services is not associated for that reason alone. The position changes if that adviser or firm is entrusted with performing activities for or on the organisation's behalf, such as administering processes, engaging customers or representing the organisation externally – different services from the same third party can produce different conclusions.

Other intermediaries may include brokers, introducers, outsourced sales teams, claims administrators and businesses operating within multi-tier delivery arrangements. Distance from the organisation does not by itself remove risk. Where such parties perform services on its behalf, organisations should consider the authority granted, customer interactions, incentive arrangements, subcontracting practices, and oversight – the assessment should focus on activities and relationships, not the number of contractual steps involved.

The practical lesson is that fraud-prevention boundaries cannot end with the payroll. An organisation should understand the network of people and entities through which it conducts business and identify those performing services for or on its behalf. This does not mean every supplier, adviser or contractor becomes an associated person; it means each material relationship should be assessed on its substance, with prevention measures proportionate to the risk it creates.

Suppliers and the Supply Chain – Where Does Responsibility End?

Supply chains require careful analysis because the legislation does not automatically treat every supplier as an associated person. A business that merely sells goods to an organisation is not associated simply because it sits within that organisation's supply chain. The position can change where a supplier also performs services for or on behalf of the organisation. Hence, liability depends on the substance of the activity rather than the existence of a purchasing relationship.

Contractors may fall within the associated-person definition when they perform services on the organisation's behalf, particularly when they interact with customers, administer transactions, or deliver outsourced functions. The contractual description is not decisive. A contractor described as independent may still qualify if the surrounding circumstances show it was performing services for or on behalf of the relevant organisation at the time the fraud occurred.

Prime contracting arrangements add complexity because delivery may pass through several organisations. A prime contractor may engage subcontractors to perform elements of a service that ultimately supports the relevant body's obligations. Government guidance recognises that a person can be an associated person without contracting directly with the relevant body, so organisations must understand which parties in extended delivery chains may actually be performing services on their behalf.

Agency relationships create particularly direct exposure. An agent authorised to negotiate, make representations, or enter into contracts on behalf of an organisation operates much more closely to it than a conventional supplier. Fraudulent statements made within that authorised activity could engage the failure-to-prevent regime where the remaining statutory conditions

are met, so organisations should scrutinise authority, remuneration, incentives and permitted external representations.

An organisation's practical ability to control distant subcontractors may nevertheless be limited. Government guidance acknowledges that a relevant organisation may exercise direct control only over its immediate contractual counterparty. A proportionate response may involve placing fraud-prevention requirements on the prime contractor and requiring similar obligations to flow down the chain, addressing due diligence, training, reporting and cooperation with any investigation.

Contractual flow-down provisions should not substitute for understanding the supply chain itself. Reasonable prevention depends on risk assessment, proportionate due diligence, and controls that reflect how services are actually delivered. Higher-risk arrangements may warrant deeper scrutiny of subcontractors, ownership, competence, incentives and prior misconduct, so that fraud-prevention measures extend far enough to cover situations in which associated persons act on the organisation's behalf.

The Intention to Benefit the Organisation

For the failure-to-prevent offence, the associated person need not succeed in producing a benefit for the organisation. The underlying fraud may be complete before any money, business or advantage is obtained. The critical issue is the associated person's intention when committing the fraud: if the conduct was intended, directly or indirectly, to benefit the organisation, the statutory condition can be satisfied even where the anticipated benefit never materialises.

The intended benefit can be financial but need not be immediate profit or revenue. Fraud intended to secure a contract, preserve a relationship, improve reported performance or obtain preferential treatment may fall within scope. Government guidance also recognises that disadvantaging a competitor can constitute an indirect benefit, so the concept extends well beyond situations in which fraudulent conduct directly places money into the organisation's accounts.

Personal motivation does not necessarily remove corporate exposure. An associated person may act primarily to secure a bonus, commission or promotion while simultaneously intending the organisation to benefit. A salesperson who dishonestly inflates sales figures to enhance personal commission is the clearest example: when personal gain is the dominant motive, the organisation is an intended beneficiary if the employee understood that the fraud would improve corporate results.

Assessment of intended benefit therefore focuses on the circumstances existing when the fraud was committed; later events do not necessarily alter that analysis. An organisation may ultimately repay money, lose the contract or suffer reputational damage and still have been the intended beneficiary at the relevant time. Compliance arrangements should identify situations in which employees might perceive fraud as advancing both personal and organisational interests.

When Fraud Benefits a Client

The failure-to-prevent regime extends beyond fraud intended to benefit the organisation itself. Section 199 also captures circumstances in which an associated person commits fraud intending to benefit a person to whom services are provided for or on behalf of the organisation, or a subsidiary undertaking of that person. Government guidance commonly describes such recipients as clients, though the legislation uses broader language than a conventional client contract.

This aspect is particularly significant for organisations whose personnel act on behalf of customers rather than merely selling products to them. Professional services firms, financial institutions, outsourced providers and administrators may place employees or agents in positions where their actions confer advantages on clients. Fraud committed in that capacity

can create corporate exposure even where the organisation itself does not stand to receive the principal benefit.

A professional adviser might dishonestly manipulate information or make false representations while acting on the organisation's behalf, with the intention of improving a client's commercial position, such as in a valuation or due diligence report. An outsourced administrator might falsify records to increase a client's entitlement or conceal non-compliance. These examples show why client-facing service models require fraud-risk assessment beyond conduct designed solely to enrich the organisation.

The statutory protection for organisations that are themselves victims is important. Section 199(3) prevents liability under the client-benefit limb where the relevant organisation was the victim, or intended victim, of the underlying fraud. Government guidance indicates this applies where the loss caused or intended by the fraud would be borne by the organisation, or where the fraud was committed with intent to harm it.

The victim exception is narrower than simply showing that the organisation suffered adverse consequences. An organisation does not become a victim merely because discovery of the fraud damages its reputation or exposes it to regulatory scrutiny. The inquiry concerns the underlying fraud itself: where an associated person intended the client to benefit while deliberately causing the organisation a loss, the exception may apply; indirect reputational consequences do not.

Financial services and outsourcing arrangements illustrate why the distinction matters. Employees may administer funds, claims or regulated processes for customers whose economic interests differ from the service provider's own. UK Finance recorded 3.13 million confirmed cases of unauthorised fraud in 2024, with losses of £722 million. Where employees or intermediaries process such claims dishonestly for a client's benefit, that conduct could create ECCTA exposure where the statutory conditions are satisfied.

The broader compliance implication is that fraud-risk assessments should examine not only how the organisation might benefit from dishonest conduct, but also how clients and other service recipients could benefit. Incentives, contractual obligations and client demands may all influence behaviour. Effective procedures should make clear that advancing a client's interests never justifies fraud, and should provide escalation routes for staff who encounter pressure to manipulate records.

Which Fraud Offences Are Covered?

The failure-to-prevent offence does not apply to every form of dishonest conduct. It applies to the fraud offences specified in Schedule 13 of ECCTA, together with aiding, abetting, counselling or procuring their commission. The underlying offence is described in official guidance as the "base fraud". Schedule 13 can be amended through secondary legislation under section 200, allowing the statutory list to develop over time.

For England and Wales, Schedule 13 includes fraud under section 1 of the Fraud Act 2006, covering fraud by false representation, fraud by failing to disclose information where there is a legal duty to do so, and fraud by abuse of position. It also includes obtaining services dishonestly under section 11 and participating in a fraudulent business carried on by a sole trader under section 9, linking the corporate offence to established Fraud Act concepts.

Other specified offences broaden the regime beyond the Fraud Act itself. Schedule 13 includes false accounting and false statements by company directors under the Theft Act 1968, fraudulent trading under section 993 of the Companies Act 2006, and the common-law offence of cheating the public revenue. Equivalent provisions and common-law offences apply in Scotland and Northern Ireland, so the framework operates across all three UK criminal-law jurisdictions.

Including secondary participation matters. A person need not personally carry out every element of the principal fraud for the conduct to be relevant; aiding, abetting, counselling or

procuring a Schedule 13 offence under section 199(6)(b) can itself constitute a qualifying base fraud. Organisations should therefore consider the risk posed by employees or intermediaries who facilitate or arrange fraudulent conduct by others, not only by those who make the final dishonest representation.

Schedule 13 provides the bridge between established fraud law and the new corporate accountability regime, without replacing the underlying offences. The associated person remains personally responsible for their own fraud, while the qualifying organisation faces a separate question about its failure to prevent it. The practical emphasis shifts from relearning fraud mechanics towards identifying where those offences could arise through business activities and who might commit them.

Fraud by False Representation in the Corporate Environment

Fraud by false representation is especially relevant to corporate activity because organisations depend on representations made to customers, contracting authorities, lenders, investors and regulators. Under the Fraud Act 2006, the offence concerns dishonest false representations made with intent to make a gain or cause, or expose another to, loss. Under ECCTA, the corporate question becomes whether such conduct by an associated person was intended to benefit the organisation or a client.

Public procurement provides an obvious example. A bidder might knowingly exaggerate experience, staffing, financial capacity or previous performance to satisfy selection criteria or improve evaluation scores. The Procurement Act 2023 tightened supplier due diligence obligations across the public sector precisely because false references, invented case studies, or inaccurate declarations can create serious risk when an associated person acts dishonestly to improve the organisation's prospects of winning business.

Certifications and compliance statements create similar exposure. An associated person might falsify professional accreditations, product testing, insurance information or cyber-security credentials to obtain or retain business. The document itself need not be elaborate; the risk arises from the dishonest representation and the intended gain or loss. Organisations should control who may make formal external declarations and ensure material claims are supported by accurate, current evidence.

Performance reporting creates risk both after contract award and during competition. Employees might manipulate service-level results, delivery statistics or social-value achievements to avoid deductions, secure incentive payments or preserve renewal prospects. Similar issues arise where customer information is altered to justify charges. Fraud prevention should therefore cover contract management and operational reporting, not only representations made during tendering or initial customer acquisition.

Environmental and sustainability claims form an increasingly important category. Fabricated emissions reductions, recycling figures, or carbon performance data could be used to secure contracts, subsidies, or a reputational advantage. Where such statements are knowingly dishonest and satisfy the underlying offence, they may create a failure-to-prevent exposure if made by an associated person with the intention of organisational benefit – controls should therefore treat non-financial claims with the same seriousness as commercial or accounting statements.

Not every inaccurate corporate statement constitutes fraud. Mistakes, optimistic forecasts and genuinely disputed interpretations require different analysis from dishonest false representations. Risk arises where associated persons dishonestly present information with the intention of obtaining prohibited gain or avoiding loss. Organisations should therefore combine verification, approval controls, and evidence retention with a culture that discourages employees from using commercial pressure to justify misleading external parties.

False Invoicing, Accounting and Financial Manipulation

False invoicing can operate in two fundamentally different directions. A fictitious invoice

submitted by an outsider to steal from an organisation ordinarily makes the organisation the victim rather than the beneficiary. By contrast, an employee or associated service provider might create inflated invoices for customers or funders intending to increase revenue. The same document type can therefore carry different ECCTA consequences depending on who acts and whom the fraud is intended to benefit.

Manipulation of accounting records presents equally serious risk. False entries, concealed liabilities, premature revenue recognition or fabricated transactions may be used to improve reported performance, satisfy lending conditions or secure investment. Tesco's 2014 accounting scandal, in which suppliers' commercial-income payments were recorded before they were due, overstated half-year profits by £326 million and ultimately cost the retailer £235 million in fines, costs and investor compensation.

Schedule 13 expressly includes false accounting under the Theft Act 1968, and the Tesco case demonstrates how such conduct fits the ECCTA framework: the underlying misstatement was designed to make the company's financial position appear stronger, directly benefiting the organisation's reported results. Where an associated person commits the relevant offence with the intention of benefiting a qualifying organisation, the failure-to-prevent framework may now operate alongside liability for the underlying accounting misconduct.

Claims and reimbursement processes generate comparable exposure. Employees or intermediaries might inflate quantities, labour hours or entitlement figures submitted to customers, public authorities or grant providers, with supporting documents altered to make an inaccurate claim appear legitimate. Prevention measures should address source-record integrity, authorisation and independent verification, particularly where those generating claims also benefit personally from revenue or performance targets.

Procurement Fraud – When Winning the Contract Creates the Risk

Procurement creates particular exposure because competitive processes depend heavily on bidders' representations about capability, experience, pricing and compliance. An associated person who dishonestly manipulates those representations to secure a contract may intend a direct commercial benefit for the organisation. Fraud risk therefore exists both before award and during delivery, requiring scrutiny of how tender strategies, approvals and submissions are developed, verified and authorised.

False tender information can take many forms, including invented references, overstated staffing, fabricated accreditations, concealed conflicts or inaccurate declarations about previous performance. Similar risks arise where employees manipulate pricing assumptions, suppress material qualifications or provide knowingly false answers to mandatory questions. Where such conduct satisfies a specified fraud offence and is intended to improve the organisation's competitive position, the failure-to-prevent regime becomes directly relevant.

The Ministry of Justice's electronic-tagging contracts show how procurement fraud plays out in practice. Serco Geografix Ltd accepted a 2019 deferred prosecution agreement, paying a £19.2 million penalty plus £3.7 million costs, after misleading the MoJ about profits from 2010 to 2013. G4S Care and Justice Services followed in 2020 with a £38.5 million penalty and £5.9 million costs, having overcharged for tagging offenders who were dead, abroad or already in custody.

Procurement fraud risk does not end when a contract is awarded. During delivery, associated persons may falsify performance data, inflate quantities or misrepresent compliance to avoid deductions, secure payments or support an extension. Contract managers may face pressure to conceal failures that could jeopardise renewal. Government guidance recommends considering fraud risk throughout the procurement lifecycle, including pre-tender activity, tendering, contract management, delivery and extensions.

Internal assistance can create additional risk when employees improperly influence procurement activity for organisational benefit – concealing disqualifying information,

coordinating misleading responses or facilitating false evidence intended to satisfy a customer's requirements. Although bribery, collusion and conflicts may fall within separate legal regimes, the failure-to-prevent offence can be relevant wherever the underlying conduct constitutes a Schedule 13 fraud intended to benefit the organisation or a client.

Effective procurement controls should combine commercial challenge with evidential discipline. High-risk submissions may require independent verification of key claims, clear ownership of tender declarations, controlled approval routes and retention of supporting evidence. Contract management data should be auditable, and any suspicious pressure to alter records should be escalated. The objective is not to obstruct legitimate competition, but to prevent commercial ambition from becoming a rationale for dishonesty.

Sales Targets, Bonuses and Commercial Pressure

Commercial incentives can influence behaviour long before fraud becomes visible. Revenue targets, commission arrangements and growth expectations may encourage employees or agents to pursue transactions aggressively, particularly where personal reward depends on short-term results. Government guidance specifically identifies reward and recognition systems as matters for fraud-risk assessment, since incentives can motivate associated persons to misrepresent products, customers, performance or compliance in ways intended to benefit the business.

The risk is not confined to obviously excessive bonuses. Ordinary performance management creates pressure when targets are unrealistic, deadlines inflexible, or failure carries serious consequences for pay or continued employment. The ACFE's 2024 global study found that fraud was linked to weak internal controls or management override of controls in more than half of the cases examined, suggesting that pressure and poor oversight compound one another rather than acting independently.

Sales environments provide clear examples. An employee might exaggerate product capabilities, omit material limitations or make false statements to close transactions before a reporting deadline. An intermediary paid primarily through commission may experience similar incentives. Where such representations satisfy an underlying fraud offence and are intended to increase revenue or protect market share, the organisation's incentive architecture becomes directly relevant to the reasonableness of its prevention procedures.

Financial and operational pressure can arise from events beyond routine sales activity – mergers, financing exercises, licence applications, grant submissions or contract renewals may create strong incentives to present results favourably. Government guidance asks organisations to consider these pressures expressly when assessing motive. Temporary periods of heightened commercial significance may justify additional controls or closer supervision, rather than reliance on procedures designed for normal operating conditions.

Workload and time pressure also matter, because employees may begin by cutting procedural corners before progressing to dishonest conduct. Under-resourced teams, unrealistic turnaround requirements or poorly designed approval systems can weaken verification and encourage expedient decisions. A fraud-prevention framework should therefore consider whether operational conditions make fraudulent behaviour more likely, particularly when a single individual prepares, approves, and benefits from a transaction without meaningful challenge.

Well-designed incentives should support sustainable performance rather than reward outcomes regardless of method. Organisations may review commission structures, introduce quality or compliance measures, apply clawback arrangements where appropriate and ensure that misconduct affects performance assessment. Senior management should also examine whether informal messages undermine formal controls: a written anti-fraud policy has limited value if employees believe that missing a target is treated more seriously than achieving it through dishonesty.

When Corporate Culture Becomes Part of the Evidence

Corporate culture can determine whether isolated misconduct remains exceptional or becomes normalised. Government guidance refers to "ethical fading", where fraudulent behaviour is gradually rationalised by beliefs that competitors behave similarly or that questionable practices are necessary to protect jobs and contracts. Such attitudes weaken formal controls because employees stop recognising unacceptable conduct, so organisations should assess assumptions and everyday behaviour, not only written policy.

Management behaviour is particularly important because employees take cues from what leaders reward, tolerate or ignore. A board may formally prohibit fraud while middle managers encourage staff to circumvent controls or avoid asking difficult questions. Communication must be consistent across all management layers; if commercial success is celebrated regardless of the method, employees may interpret silence about questionable practices as approval, even if the written policy states otherwise.

Whistleblowing arrangements provide another indicator of culture. Cifas's Fraudscape 2026 report recorded 288 subjects filed to its Insider Threat Database in 2025, a 21% increase on the previous year, with dishonest action by staff to obtain a benefit the most common case type. Organisations that protect those who raise concerns and respond visibly to substantiated misconduct can reduce rationalisation and improve early detection.

Culture can also become evidentially relevant when an organisation seeks to demonstrate that its procedures were reasonable. Policies and training records may show formal compliance, but their credibility is undermined where actual conduct reveals tolerance for dishonesty. Consistent disciplinary action, ethical leadership and transparent escalation support the opposite conclusion. Effective governance therefore requires alignment between documented expectations and the behaviour actually rewarded in practice.

The Reasonable Fraud-Prevention Procedures Defence

The failure-to-prevent offence contains a statutory defence under section 199(4) that places prevention procedures at the centre of corporate exposure. A relevant organisation can defend proceedings by proving that, when the base fraud occurred, it had reasonable procedures to prevent associated persons committing fraud of that kind – or that, in all the circumstances, it was reasonable not to have any. The defence, therefore, depends on context rather than on a universal checklist.

The burden of establishing the defence rests with the organisation, which must prove it on the balance of probabilities. This matters because the prosecution need not prove the organisation's procedures were unreasonable once the statutory offence is otherwise made out; the organisation must instead demonstrate the quality and relevance of its own prevention framework, making contemporary records crucial to showing which risks were identified and how they were addressed.

Reasonableness does not require every possible control to be implemented. Government guidance adopts an outcome-focused, proportionate approach, recognising differences in organisational size, complexity and exposure. A control appropriate for a regulated financial institution may be unnecessary for a lower-risk business. At the same time, a simple policy may be inadequate for an organisation using numerous agents or intermediaries. The key question is whether procedures were reasonable for the fraud risks actually faced.

The alternative argument – that it was reasonable to have no preventive procedures – should be approached with caution. Government guidance recognises the statutory possibility, but an organisation would need to justify that conclusion by reference to its own circumstances and assessed risks. Where no procedures are adopted, the reasoning should be documented and reviewed; an unexamined assumption that fraud is unlikely may be difficult to defend later.

Implementation is as important as design. Procedures that exist only on paper provide limited protection if employees are unaware of them, managers routinely bypass them, or breaches

carry no consequence. Reasonable procedures should therefore be accessible, understood, properly resourced and enforced. Evidence of training, due diligence, monitoring, and management response can help demonstrate that the framework operated in practice rather than merely functioned as a formal compliance document.

The Six Principles of Fraud Prevention

Government guidance, published on 6 November 2024, organises reasonable fraud prevention around six principles: top-level commitment, risk assessment, proportionate risk-based prevention procedures, due diligence, communication including training, and monitoring and review. These mirror the framework already used for the Bribery Act 2010 and the Criminal Finances Act 2017's tax-evasion facilitation offence, so many large organisations should already have foundations of relevant practice in place.

The principles are deliberately flexible and outcome-focused rather than prescriptive; following them mechanically does not guarantee a defence. Instead, they offer a structure through which an organisation designs, implements and evidences procedures proportionate to the fraud risks posed by its activities and associated persons. Top-level commitment sets expectations, risk assessment identifies exposure, and the remaining principles translate that assessment into operational practice.

The principles are interdependent, and a weakness in one can undermine the others. Extensive training achieves little if risk assessment fails to identify the relevant fraud scenarios, while sophisticated due diligence cannot compensate for leaders who tolerate dishonest commercial behaviour. Controls that were proportionate when introduced may become inadequate after acquisitions, new markets or changes in delivery models, so the components must be considered collectively rather than in isolation.

The six principles also reinforce proportionality. The same prevention framework will not suit every organisation or every associated person; higher-risk sales agents may justify enhanced due diligence and closer monitoring, while low-risk service relationships may need fewer controls. Proportionality should nevertheless rest on documented assessment rather than convenience, with organisations able to explain why particular procedures were selected, strengthened, reduced or considered unnecessary.

The framework is best treated as a cycle rather than a one-off project. Leadership informs risk assessment; assessment drives prevention measures; due diligence and communication support implementation; monitoring identifies weaknesses; and review feeds new information back into governance. This ongoing process helps organisations adapt to changing fraud typologies and commercial pressures, while creating the evidence needed to show that prevention arrangements remained reasonable over time.

Top-Level Commitment – Fraud Prevention Starts with Governance

Government guidance places top-level commitment first because fraud prevention depends on the attitude of those who govern and manage the organisation. Boards, partners and senior management should be committed to preventing associated persons from engaging in fraud. They should foster a culture in which fraudulent conduct is never acceptable, including a willingness to reject profit, contracts, or other commercial advantages that are based on or assisted by fraudulent behaviour.

Top-level commitment requires more than approving an anti-fraud policy. Governance arrangements should identify who owns fraud risk, how information reaches senior decision-makers, and which committees oversee prevention activity. Appropriate resources should be provided for risk assessment, training, due diligence and investigation. Responsibility can be delegated operationally, but leadership should retain sufficient visibility to identify weaknesses and ensure remediation when controls prove ineffective.

The board or an equivalent governing body should receive information sufficient for meaningful oversight, including significant fraud risks, whistleblowing themes, investigation outcomes,

high-risk third parties and overdue remediation. Reporting should distinguish fraud against the organisation from fraud intended to benefit it or its clients, because the latter presents the distinctive ECCTA exposure. Management information showing whether prevention arrangements actually function strengthens governance more than confirming that policies merely exist.

Senior leaders also shape the incentive environment. Decisions about targets, commissions, budgets and staffing can increase or reduce fraud risk even when not presented as compliance matters. Leadership should challenge whether commercial expectations create pressure to manipulate information or circumvent controls, since messages that fraud is unacceptable must be reflected in remuneration and disciplinary decisions, or employees may conclude that results matter more than how they were achieved.

Visible response to misconduct is another element of credible commitment. Where investigations substantiate fraudulent behaviour, organisations should apply appropriate consequences and address underlying control weaknesses, without seniority or commercial success shielding individuals from scrutiny. Lessons may need to be communicated more widely so that staff understand both the organisation's standards and the consequences of a breach, since consistency between stated values and actual responses strengthens the cultural foundation for reasonable procedures.

Good governance treats fraud prevention as a continuing responsibility rather than a narrow compliance function. The board should periodically reassess whether the organisation's risk profile, associated-person population and control environment have changed, since major acquisitions, new markets or restructuring can significantly alter exposure. Top-level commitment is most convincingly demonstrated when leadership anticipates these changes and requires that fraud risk be considered in ordinary strategic decision-making.

Fraud Risk Assessment – Understanding How the Organisation Could Benefit

Fraud risk assessment under ECCTA requires organisations to examine a category of risk that traditional internal-fraud exercises may overlook. Many established controls focus on employees stealing money, assets or data from the organisation. The failure-to-prevent offence requires additional attention to fraud committed by associated persons for the organisation's benefit, or in relevant circumstances a client's benefit, so the assessment must look outward as well as inward.

Government guidance states that risk assessment should be dynamic, documented and kept under regular review. Organisations may extend existing economic-crime assessments, but should ensure the specific ECCTA exposure is addressed. Mapping associated persons provides a useful starting point, particularly for agents, outsourced workers and employees in sensitive roles; each activity should then be examined for opportunities, motives and rationalisations that could lead to fraudulent behaviour.

Opportunities may arise wherever individuals can make external representations, control financial information, submit claims or approve transactions without sufficient challenge. Motive can be created by bonuses, targets or upcoming commercial events, while rationalisation develops where dishonest practices are considered normal. Examining these three dimensions helps organisations move beyond generic fraud registers towards scenarios that reflect how misconduct could realistically occur within their own operating model.

The assessment should also consider change. Acquisitions, new products, unfamiliar jurisdictions, new intermediaries and major tenders can create fraud opportunities that did not exist previously, and internal investigations, whistleblowing and audit findings should feed back into the process. A risk assessment that remains unchanged despite significant business change provides weak evidence of reasonable procedures, because prevention measures cannot stay proportionate to risks that have not been reassessed.

Proportionate Controls – Prevention Rather Than Paper Compliance

Reasonable fraud-prevention procedures should reflect the nature, scale, and complexity of the organisation, as well as the risks identified through its own assessment. A multinational group using extensive sales agents may require substantially different controls from a simpler organisation with limited external representation. Proportionality does not mean minimal compliance; it means selecting measures strong and well-supervised enough to reduce realistic fraud scenarios to an appropriately managed level.

Government guidance emphasises that procedures should be clear, practical, accessible and effectively enforced. Controls that exist only in policy documents provide limited protection if employees cannot understand them, managers routinely bypass them, or breaches produce no meaningful consequences. Procedures should operate within ordinary business processes, with responsibilities clearly assigned and exceptions subject to genuine scrutiny rather than informal workarounds driven by commercial convenience.

Existing compliance frameworks can provide a useful foundation. Financial controls, anti-bribery procedures, procurement rules and internal audit programmes may already address elements of fraud risk. Organisations should not assume, however, that controls built for different purposes automatically satisfy the ECCTA standard; each framework should be tested against fraud committed by associated persons for organisational or client benefit to identify where adaptation or stronger implementation is needed.

Control design should distinguish preventative and detective measures. Segregation of duties, approval limits and verification requirements may prevent misconduct, while audits, exception reports and whistleblowing mechanisms may identify it after it begins. Effective frameworks usually combine both approaches, since no single control is infallible; organisations should consider how quickly suspicious activity could be detected and whether escalation allows intervention before fraud becomes systemic.

Proportionate procedures should remain explainable. If a control is omitted, reduced or applied only to particular business areas, the organisation should be able to demonstrate the reasoning behind that decision and its connection to assessed risk. This evidential discipline helps prevent proportionality from becoming a retrospective justification for weak controls; a defensible prevention framework is one whose design, implementation and enforcement follow a documented understanding of actual exposure.

Due Diligence on Suppliers, Agents and Business Partners

Due diligence is a central component of reasonable fraud prevention because associated persons can expose an organisation through activities performed on its behalf. The appropriate level of scrutiny should be risk-based rather than uniform, considering the services performed, authority granted, access to customers or funds, geographical exposure, remuneration structure, and the extent to which the third party can make representations that create financial or commercial benefit.

Initial screening may consider trading history, professional or regulated status, ownership, directors, financial standing and publicly available information about misconduct or enforcement action. Internet searches, specialist screening tools and third-party risk platforms may assist where proportionate. The purpose is not to eliminate every conceivable risk, but to identify indicators that justify deeper enquiry, additional contractual protection, or a decision not to appoint an unacceptably risky party.

Ownership and control can be particularly important where intermediaries operate through opaque structures or undisclosed relationships that may create conflicts of interest. Organisations may need to understand ultimate beneficial ownership and connections with employees, customers or public officials where relevant to risk. A declaration of interests can support that process, but should not automatically replace independent verification where the relationship's nature or value warrants further scrutiny.

Contracts should reinforce the conclusions reached through due diligence. Appropriate

provisions may require compliance with anti-fraud standards, accurate recordkeeping, prompt notification of suspected misconduct, cooperation with investigations and termination rights for serious breaches. Agent agreements deserve particular attention because agents can make representations or negotiate externally on the organisation's behalf, and contractual protections work best when responsibility for monitoring compliance is clearly assigned.

Due diligence should continue beyond onboarding, because relationships and risks change materially over time. A previously low-risk contractor may expand into customer-facing work, use new subcontractors or experience ownership changes. Renewal, extension, material scope changes, and significant incidents should provide opportunities for reassessment, with periodic review appropriate for higher-risk associated persons whose activities create ongoing exposure over the course of a long contractual relationship.

Effective due diligence combines information gathering, judgement and follow-through. Organisations should record what was checked, what concerns arose, how they were resolved and why the resulting level of control was considered proportionate. Where red flags are knowingly accepted, that decision should be explainable later. Hence, the process supports informed commercial decision-making rather than becoming a mechanical collection of documents never evaluated against actual fraud risk.

Mergers and Acquisitions – Buying Someone Else's Fraud Risk

Mergers and acquisitions can transfer fraud risk along with assets, customers and revenue. Pre-acquisition due diligence should examine whether the target has faced fraud allegations, internal investigations, regulatory action or material whistleblowing concerns. Historical misconduct may reveal weaknesses in culture or control that remain relevant after completion, and buyers should consider whether the target's business model relies on agents or practices creating heightened exposure under the failure-to-prevent regime.

Financial and tax information can provide further indicators. Unusual revenue recognition, unexplained adjustments, aggressive accounting positions or irregular payments may justify deeper investigation, echoing the accounting irregularities that ultimately cost Tesco £235 million in 2017. Due diligence should also consider the target's own fraud risk assessments, prevention procedures and internal audit findings, to understand whether the acquiring organisation could inherit inadequately controlled operations.

Incentive arrangements deserve particular attention because acquisition targets may operate remuneration structures that are materially different from those of the buyer. Commission-heavy models, exceptional growth targets, or management rewards closely tied to short-term financial results may increase pressure to manipulate information. Whistleblowing arrangements should also be assessed, since the absence of reported concerns is not necessarily reassuring when employees lack trusted channels to speak up.

Post-acquisition integration is equally important. Government guidance identifies both M&A due diligence and post-acquisition integration of fraud-prevention measures as relevant best practice. Newly acquired businesses should be incorporated into the group's risk assessment, governance, training and monitoring arrangements within a proportionate timeframe, with interim controls applied where weaknesses are identified, so acquisition activity does not create a prolonged period of unmanaged fraud risk.

Contracts as a Fraud-Prevention Control

Contracts translate an organisation's fraud-prevention expectations into obligations binding suppliers, agents, contractors and other business partners. Appropriate clauses may prohibit fraudulent conduct, require compliance with relevant policies and oblige counterparties to maintain proportionate procedures of their own. Representations and warranties can also address the accuracy of information provided during procurement or onboarding, establishing clear consequences for appointments secured through false or misleading statements.

Record-keeping obligations strengthen prevention and investigation by requiring associated

persons to maintain accurate, auditable information to support invoices, claims, and performance reports. Contracts may also provide audit or inspection rights, allowing the organisation to test compliance where risk justifies it. Such rights should be drafted realistically; an extensive audit clause provides little value if the organisation lacks the authority, resources or willingness to exercise it when warning signs arise.

Notification provisions may require prompt reporting of suspected fraud, investigations, or control failures affecting the relationship, while cooperation clauses may oblige the counterparty to preserve evidence and assist with enquiries. These provisions can be particularly valuable within outsourced operations the organisation cannot investigate directly, since clear escalation requirements reduce the risk that material concerns remain confined within a supplier's own management structure until substantial damage occurs.

Subcontracting arrangements may require contractual flow-down provisions extending fraud-prevention expectations beyond the prime contractor. A relevant organisation may not have a direct agreement with every subcontractor, but can require its counterparty to impose specified obligations further down the delivery chain, addressing due diligence, training, recordkeeping, and cooperation, while reserving the right to approve or challenge subcontractors engaged in particularly sensitive activities.

Termination and suspension rights provide important remedies where serious fraud concerns arise, but should be proportionate and carefully drafted. Immediate termination may be warranted for established fraudulent conduct, while suspected misconduct may require an investigation first. Organisations should consider whether contracts permit the suspension of particular activities, the withholding of disputed payments, or the replacement of personnel, so that remedies support risk management without creating obligations that are commercially unrealistic to apply fairly.

Contract wording alone does not establish reasonable procedures. Obligations must be communicated, monitored and used when circumstances require. If an organisation routinely ignores reporting failures, never reviews required records, or fails to renew high-risk suppliers despite unresolved concerns, strong drafting has little evidential value. Contracts should therefore form one component of a wider framework incorporating due diligence, relationship management and escalation, so protections operate in practice rather than remaining standard terms on paper.

Procurement and legal teams should align contractual requirements with the fraud risks identified for each relationship. Standard clauses provide consistency, but higher-risk arrangements may warrant enhanced controls, whereas low-risk relationships may not require the same level of intervention. The organisation should be able to explain why particular protections were selected and how compliance is overseen, making contracting a practical prevention tool rather than an isolated legal exercise disconnected from operational delivery.

Training, Communication and Speaking Up

Fraud-prevention training should reflect the responsibilities and exposure of the people receiving it. Generic annual awareness modules establish basic principles but are unlikely to address every material risk. Procurement teams may need guidance on false tender information and supplier representations; sales teams may require scenarios involving mis-selling and incentives; while finance, contract management, and senior leadership face different opportunities for misconduct and should understand the controls relevant to their own decisions.

Training should explain not only prohibited conduct but the circumstances in which legitimate commercial behaviour can cross into fraud. Employees may understand that falsifying an invoice is wrong yet fail to recognise the seriousness of manipulating performance data or withholding material information during a tender. Practical scenarios can make those boundaries clearer, and refresher training should respond to changes in risk, investigations and regulatory developments rather than repeating the same material each year.

Communication should extend beyond employees where associated persons outside the organisation create material risk. Agents, contractors and other intermediaries may need relevant policies, contractual expectations or targeted briefings, with the level of engagement kept proportionate to their role. A third party authorised to make representations to customers may require substantially more detailed communication than a low-risk supplier whose activities create little realistic opportunity for fraud that would benefit the organisation.

Speaking-up arrangements support prevention by allowing concerns to surface before misconduct becomes entrenched. Channels should be accessible, trusted and capable of handling reports independently from managers who may themselves be implicated. Cifas recorded a record 444,993 fraud-risk cases across its National Fraud Database in 2025, and its members reported preventing £2.4 billion in losses that year – figures that depend heavily on individuals inside organisations being willing and able to raise concerns.

Communication is most effective when leadership behaviour supports the message. Staff may disregard training if managers routinely instruct them to bypass controls or treat questionable practices as commercially necessary. Organisations should reinforce anti-fraud expectations through management briefings, performance discussions, and incident responses. Training records and attendance data provide useful evidence, but their real value depends on whether employees actually understood and applied the relevant requirements.

Governance, Records and the Audit Trail

The reasonable-procedures defence has an important evidential dimension, because an organisation may need to demonstrate what it knew, what it assessed and why particular decisions were taken before the fraud occurred. Contemporary records show that fraud risk was considered systematically rather than reconstructed after an investigation began. Risk assessments, committee papers, due diligence files, and monitoring reports may collectively demonstrate how the organisation identified exposure and responded with proportionate measures.

Governance records should identify responsibility for key decisions. Where a significant control is introduced, reduced or removed, documentation should explain the rationale and the authority approving the change. The same applies to exceptions from normal procedures: informal dispensations become difficult to defend if nobody can establish who authorised them or why, whereas clear decision records strengthen accountability and allow future reviewers to understand the circumstances at the time the judgement was made.

Government guidance specifically recommends documenting decisions in which organisations conclude that particular preventative measures are unnecessary, and recording who authorised them. This matters because the statutory defence can include circumstances in which it was reasonable not to have certain procedures at all. A documented, evidence-based conclusion reached after proper assessment is materially different from an absence of controls caused by oversight, inertia or an unsupported belief that fraud is unlikely.

Training and communication should also leave an appropriate audit trail. Organisations may need to establish who received relevant training, when it occurred, what subjects were covered and whether high-risk groups received additional instruction. Records of policy circulation and external communication support the same purpose. Attendance alone does not prove effective prevention, but its absence makes it harder to demonstrate that procedures were embedded rather than issued centrally.

Due-diligence and monitoring records provide further evidence of implementation. Screening outcomes, red flags, approval decisions, supplier reviews and remediation actions can show that controls operated over time. Where concerns were identified, records should establish how they were investigated and resolved; a pattern of unresolved findings may itself reveal weakness, particularly if senior management received warnings but allowed commercially important relationships to continue without strengthening oversight.

The audit trail should capture both reasoning and activity. Large volumes of documents are not persuasive on their own if they do not explain how risk influenced decisions. Effective governance records connect identified risks to controls, responsibilities, reviews and remediation, a connection that may become important evidence during any investigation or prosecution. Good record-keeping is not bureaucratic decoration; it demonstrates whether fraud prevention was part of real organisational decision-making.

Monitoring, Testing and Continuous Review

Fraud-prevention arrangements cannot remain static, because organisations, associated-person relationships and fraud techniques all change. Government guidance expects monitoring and review to identify weaknesses and support improvement. A procedure that was reasonable when introduced may become inadequate after growth, restructuring, or expansion into new markets, so organisations should establish mechanisms to confirm that controls continue to address current exposures rather than assuming that past implementation guarantees ongoing effectiveness.

Control testing can assess whether procedures work as intended. Internal audit, compliance reviews and sample testing can identify failures in approvals, due diligence, segregation of duties or recordkeeping. Testing should examine actual transactions and behaviours rather than merely confirming that policies exist. Where controls repeatedly fail, management should determine whether the cause is poor design, insufficient resources, inadequate training, or deliberate circumvention, and record the corrective action taken.

Data analytics can identify patterns that conventional review may miss. Duplicate invoices, unusual payment timing, repeated contract variations or sudden performance improvements may justify investigation. Procurement analytics can highlight unusual bidding patterns or excessive single-source activity requiring closer examination. Analytics do not establish fraud on their own, but can flag anomalies warranting human assessment and strengthen the organisation's ability to detect emerging problems earlier.

Investigation findings and whistleblowing reports should feed directly into the prevention framework. A substantiated incident may reveal that a risk assessment omitted a realistic scenario, that training was misunderstood, or that a manager routinely overrode controls. Even unsubstantiated reports may expose confusion or weakness requiring attention. Organisations should treat investigations as sources of organisational learning, translating lessons into revised procedures, targeted communication or additional monitoring.

External developments also matter. Enforcement action, sector guidance and new fraud typologies may alter what constitutes a reasonable response. Artificial intelligence and increasingly sophisticated document manipulation create both new fraud opportunities and improved detection tools; the ICAEW has flagged the new offence's implications for statutory audit under ISA 240 and ISA 250A, meaning auditors' own inquiries into management's fraud-prevention procedures now form part of the wider assurance landscape.

An outdated risk assessment undermines the credibility of the whole framework, because prevention procedures depend entirely on the risks they address. Reviews should occur periodically and following material changes or significant incidents. The objective is not constant redesign but informed adaptation – a mature organisation should be able to show how monitoring generated findings, how those findings were evaluated, and how controls evolved once evidence showed existing arrangements were no longer sufficient.

What Happens When Fraud Is Suspected?

When suspected fraud arises, the organisation should respond promptly while avoiding premature conclusions. Clear escalation routes ensure concerns reach personnel with sufficient independence and authority to act. The initial response may involve securing records, restricting access, suspending transactions or preserving digital evidence. Decisions should be documented carefully, because early actions can affect the integrity of an

investigation and the organisation's ability to demonstrate a responsible response.

Investigations should be proportionate to the seriousness and complexity of the allegation and should avoid conflicts of interest. Internal audit, compliance, legal teams, specialist investigators, or external advisers may become involved, depending on the circumstances, with terms of reference defining scope, reporting lines, and authority. Where legal advice or anticipated litigation is relevant, organisations should seek legal advice on legal professional privilege rather than assuming that every investigation document is automatically protected.

Evidence preservation is particularly important where emails, messaging platforms or third-party records may contain relevant material. Routine deletion processes may need to be suspended and custodians informed of preservation requirements, with organisations maintaining appropriate chain-of-custody and access controls. External associated persons may also hold important records, making contractual cooperation and audit provisions valuable when the organisation needs information from suppliers, agents or outsourced providers.

Employment and contractual consequences should be considered separately from criminal conclusions. An employee may face disciplinary investigation under internal procedures, while an agent or supplier may trigger suspension, remediation or termination rights. Organisations should apply these mechanisms fairly and consistently, taking care not to destroy evidence or prejudice wider enquiries; where control weaknesses contributed to the incident, remediation should address them regardless of whether individual misconduct results in formal action.

The organisation may also need to decide whether to notify regulators, law-enforcement bodies, insurers or customers. Some reporting duties are mandatory, while voluntary self-reporting can carry real enforcement weight. The Joint SFO-CPS Corporate Prosecution Guidance, published on 18 August 2025, confirms that prompt self-reporting and full cooperation weigh heavily in favour of a deferred prosecution agreement rather than prosecution, though every case remains fact-specific.

An associated person need not be prosecuted before proceedings can be brought against the organisation. The prosecution may establish the underlying base fraud within the corporate proceedings themselves. However, where the associated person has not been prosecuted, the prosecution must still prove to the criminal standard that they committed the relevant base fraud offence – corporate liability removes the need for a prior individual conviction, but not the requirement to establish the underlying fraud.

Penalties, Prosecution and Deferred Prosecution Agreements

A conviction for failure to prevent fraud can result in an unlimited fine, with no fixed statutory ceiling; the ultimate figure depends on the circumstances and applicable sentencing principles. The impact of prosecution extends well beyond the fine itself. Organisations may face investigation costs, management disruption, reputational damage, regulatory scrutiny, and adverse reactions from customers, lenders, and investors, particularly where the offending behaviour suggests broader weaknesses in governance or culture.

Commercial consequences may also affect procurement and contracting relationships. Customers may scrutinise whether the organisation remains suitable for sensitive work, while existing agreements may contain notification, warranty, or termination provisions that are triggered by criminal proceedings or findings. Regulated organisations may face additional supervisory consequences, and insurers may examine coverage carefully. Even where business continues, substantial remediation may be needed to restore confidence and demonstrate that identified weaknesses have been corrected.

Deferred prosecution agreements provide an alternative to conventional corporate prosecution in England and Wales for specified economic crimes, including failure to prevent fraud. A DPA is an agreement between a prosecutor and an organisation under judicial supervision: criminal proceedings are instituted but suspended for an agreed period, provided

the organisation complies with specified conditions. DPAs apply to organisations rather than individuals and are not available under the corresponding Scottish or Northern Irish arrangements.

Conditions attached to a DPA can include financial penalties, compensation, disgorgement, cooperation requirements, and the implementation of compliance programmes, with judicial approval required and the court considering whether the agreement is in the interests of justice and is fair, reasonable, and proportionate. Since 2014, the SFO has concluded DPAs with organisations including Tesco Stores (£129 million), Serco Geografix (£19.2 million) and G4S Care and Justice Services (£38.5 million).

Where a company is convicted rather than offered a DPA, penalties can be far larger. Glencore Energy (UK) Ltd was convicted on seven counts of bribery in 2022 and ordered to pay £281 million – a fine, confiscation order and costs reflecting what the sentencing judge called an "endemic" culture within one trading desk. The case illustrates the scale of financial exposure that corporate conviction can create; section 250 now broadens the circumstances in which criminal conduct can be attributed to organisations of any size.

Remediation can become central to enforcement outcomes because prosecutors examine whether the organisation recognised weaknesses and responded effectively. The SFO's November 2025 guidance on evaluating corporate compliance programmes considers such programmes in the context of prosecution decisions, DPAs, potential statutory defences, sentencing and monitorships. Improvements made after misconduct cannot retrospectively create reasonable procedures at the time of the offence, but they influence how prosecutors and courts assess the organisation's subsequent response.

The enforcement regime reinforces the importance of prevention before misconduct occurs and remediation once weaknesses are discovered. As at August 2026, no organisation had yet been convicted or entered into a DPA under the section 199 failure-to-prevent-fraud offence, although the SFO has publicly signalled its readiness to use the new offence. An organisation with a documented risk assessment, functioning controls and evidence of effective implementation is materially better placed than one that ignored warning signs or failed to address identified weaknesses.

Territorial Reach – Fraud Beyond the UK's Borders

The failure-to-prevent fraud offence can apply beyond organisations established in the United Kingdom, but only where the underlying fraud has a sufficient UK nexus. Government guidance states that the associated person must commit a base fraud offence under the law of part of the UK, generally requiring that an act forming part of the fraud occurred in the UK, or that the relevant gain or loss occurred within the UK.

An overseas organisation can therefore face exposure where an employee or associated person commits fraud in the UK, or where conduct outside the UK targets victims here and produces the necessary gain or loss. The organisation's place of incorporation does not by itself prevent prosecution. Multinational groups should assess UK-facing activities and service delivery rather than assuming overseas operations fall outside scope merely because they are managed abroad.

The reverse position is equally important. A UK-based organisation is not automatically liable for every fraud committed overseas by employees, agents or subsidiaries. Where conduct occurs wholly abroad and produces no relevant UK gain or loss, the necessary nexus may be absent, and the matter may instead fall within the jurisdiction of authorities in the country where the fraud occurred or where its effects were felt.

International outsourcing can make territorial analysis particularly complex, because different stages of a transaction may occur in different jurisdictions. A service may be administered overseas, represented to a UK customer, processed through UK systems and ultimately produce financial consequences here. Organisations should examine where representations

are made, where victims are located and where gain or loss occurs, rather than relying solely on the location of the associated person.

For multinational groups, territoriality should form part of the fraud risk assessment and control design from the outset. Overseas employees and associated persons may require procedures to address UK-related activities, even where local operations are largely autonomous. At the same time, resources should not be diverted on the assumption that ECCTA governs conduct with no UK connection at all. The practical objective is to identify where cross-border business creates a realistic UK nexus.

Beyond Legal Compliance – What Good Fraud Governance Looks Like

Good fraud governance requires more than producing another policy. The central question is whether the organisation's operating model makes fraud difficult to commit for its benefit, likely to be detected, and culturally unacceptable. That requires fraud prevention to be embedded within commercial decision-making, financial control, procurement, employment practices, sales activity, and board oversight, rather than being treated as a specialist compliance subject operating apart from the rest of the business.

Procurement contributes by overseeing supplier selection, tender submissions, conflict resolution, contract terms, and the integrity of claims made during delivery. Finance provides segregation of duties, payment controls and scrutiny of unusual transactions. Sales functions must manage incentives and representations to customers, while contract-management teams verify performance data and claims. Fraud governance strengthens when these functions share information rather than each assuming another department owns the relevant risk.

Human resources also plays an important role because recruitment, remuneration, performance management, and disciplinary arrangements affect both opportunity and motive. Unrealistic targets, poorly designed bonuses or tolerance of misconduct by high performers can undermine formal controls. HR can support prevention through appropriate screening, clear behavioural expectations and consistent consequences – culture is shaped as much by how individuals are rewarded and treated as by centrally issued policies.

Compliance and legal teams provide specialist interpretation, risk challenge and advice on controls, but cannot prevent fraud alone. Operational managers remain closest to the activities in which associated persons act and should understand where dishonest conduct could benefit the organisation or its clients. Effective frameworks allocate responsibility across the business, combining central standards with local ownership so prevention becomes part of routine management rather than an externally imposed requirement.

Internal audit provides independent assurance by testing whether controls operate as management believes they do. Its findings can reveal gaps between documented procedures and actual practice, particularly where exceptions have become routine, or management overrides are common. Audit results should feed into risk assessment, remediation and board reporting, determining not simply whether technical control failures exist but whether the overall prevention framework remains proportionate to the fraud risks the organisation actually faces.

Board governance draws these elements together. Senior leaders should receive sufficient information to understand major fraud risks, significant incidents, high-risk associated persons and overdue remediation. They should challenge whether commercial strategies, acquisitions or incentive arrangements create new exposure. A board that considers fraud only after misconduct occurs is reacting too late; good governance requires fraud risk to be weighed before organisational change creates avoidable vulnerability.

The measure of effective governance is therefore practical rather than documentary. Policies, training records and contractual clauses matter, but persuade only when supported by behaviour, oversight and evidence of implementation. ECCTA encourages organisations to

demonstrate that fraud prevention is integrated into how business is conducted: risks identified, controls proportionate, concerns escalated, misconduct met with consequences, and lessons producing change – the difference between formal compliance and a credible prevention culture.

Summary – From Individual Fraud to Corporate Accountability

Traditional fraud law naturally focuses on the individual who makes a dishonest representation, falsifies an account, or abuses a position of trust. The failure-to-prevent regime adds a different question: what responsibility should fall on the organisation that stood to benefit from that conduct? ECCTA therefore shifts part of the legal focus from the individual act itself towards the corporate environment in which it was committed and the systems intended to prevent it.

That change requires organisations to look carefully at who acts on their behalf and how authority is exercised. Employees are only part of the picture; agents, subsidiary undertakings, contractors and other persons performing services for or on behalf of the organisation may also create exposure. Understanding those relationships is fundamental because effective fraud prevention depends on identifying where associated persons can make representations, control information, or otherwise create an advantage through dishonest conduct.

The intended beneficiary is equally important. Fraud need not succeed before the offence becomes relevant, and personal gain does not necessarily exclude corporate benefit. Organisations should examine where bonuses, commercial targets, customer pressures or procurement objectives might encourage individuals to rationalise dishonesty as beneficial to the business or its clients – significant risk arises wherever fraudulent behaviour appears commercially useful, particularly when management signals that results matter more than method.

Ultimately, ECCTA asks whether the organisation can demonstrate that it took reasonable steps to prevent relevant fraud before it occurred. That requires more than policies drafted after risks become apparent. Strong governance connects risk assessment, due diligence, proportionate controls, training, contracts, monitoring, and leadership into an evidence-based prevention framework, so corporate accountability now turns not only on who committed the fraud but also on whether the organisation maintained a reasonable system designed to prevent it.

With the National Audit Office estimating that fraud and error cost the UK taxpayer between £55 billion and £81 billion in 2023/24, and the typical organisation losing around 5% of annual revenue to fraud according to the ACFE, the case for treating prevention as a governance priority rather than a compliance afterthought is compelling. ECCTA gives that priority statutory force, and organisations of every size should now be able to show it is being met.

Additional articles can be found at Procurement and Supply Chain Management Made Simple. This site looks at procurement and supply chain management issues to assist organisations and people in increasing the quality, efficiency, and effectiveness of their product and service supply to the customers' delight. © Procurement and Supply Chain Management Made Simple. All rights reserved.

Further Reading

- *Economic Crime and Corporate Transparency Act 2023, c.56 – legislation.gov.uk*
- *Crime and Policing Act 2026, c.20, section 250 – legislation.gov.uk*
- *Home Office, "Crime and Policing Act 2026: serious crime factsheet" – gov.uk*
- *Home Office, "Economic Crime and Corporate Transparency Act 2023: guidance to organisations on the offence of failure to prevent fraud" (6 November 2024)*
- *Serious Fraud Office and Crown Prosecution Service, "Joint SFO-CPS Corporate Prosecution Guidance" (18 August 2025)*

- *Serious Fraud Office, guidance on evaluating corporate compliance programmes (November 2025) – sfo.gov.uk*
- *Serious Fraud Office, case summaries and statements of facts: Tesco Stores Ltd (2017); Serco Geografix Ltd (2019); G4S Care and Justice Services (UK) Ltd (2020); Glencore Energy (UK) Ltd (2022) – sfo.gov.uk*
- *Companies House, "Economic Crime and Corporate Transparency Act: transition plan" – gov.uk*
- *National Audit Office, reporting on the cost of fraud and error to the public purse, 2023/24*
- *Public Sector Fraud Authority, Annual Report 2023–24 and subsequent Parliamentary updates – gov.uk*
- *Office for National Statistics, "Fraud and computer misuse in England and Wales", year ending March 2025*
- *UK Finance, "Annual Fraud Report 2025"*
- *Association of Certified Fraud Examiners, "Occupational Fraud 2024: A Report to the Nations"*
- *Cifas, "Fraudscape 2026"*
- *Tesco Supermarkets Ltd v Nattrass [1972] AC 153 (House of Lords)*
- *Institute of Chartered Accountants in England and Wales (ICAEW), "The new 'Failure to Prevent Fraud' offence: a compliance and accounting perspective"*