DESIGNING CONTROLS WITH BEHAVIOUR IN MIND: *ADDRESSING INSIDER FRAUD IN THE PUBLIC SECTOR*

DR RASHA KASSEM,

SENIOR LECTURER IN ACCOUNTING & LEADER OF THE FRAUD RESEARCH GROUP,

ASTON UNIVERSITY

Insider fraud is one of the most damaging and underestimated risks in the public sector, often enabled by weak controls but driven by deeper human behaviours like resentment, entitlement, rationalisation, and a lack of oversight. Dr Rasha Kassem explores how public bodies can design fraud controls that consider not just what people do, but why they do it.

Insider fraud presents a growing and often under-recognised threat within the UK public sector, where the stakes of trust, transparency, and public accountability are particularly high.

In government departments, local authorities, NHS bodies, and publicly funded organisations, insider fraud occurs when individuals entrusted with public responsibility, including civil servants, local government officers, finance staff, procurement teams, or senior managers, exploit their positions to deceive the organisation for personal benefit or to advantage others.

These personal benefits may be financial, such as falsifying expense claims for personal reimbursement, diverting public funds to personal accounts or fictitious suppliers, or manipulating procurement processes to award contracts to associates or entities offering bribes.

They may also be non-financial, including gaining unauthorised access to confidential data to benefit the dear and near (e.g., friends, family, or accomplices), abusing their position by interfering in regulatory or disciplinary processes to protect themselves or close colleagues from scrutiny, securing employment or promotions for relatives or friends through nepotism, or influencing decision-making for ideological or political motives rather than objective public interest.

Some perpetrators rationalise their actions, believing they are acting in the organisation’s interest rather than for personal gain, for example, protecting jobs or preserving reputation — despite knowingly breaching ethical or legal boundaries.[1]

In all cases, insider fraud is uniquely damaging because the threat comes from within and undermines public trust, weakens service delivery, and can have long-lasting reputational and financial consequences for public bodies. According to the Association of Certified Fraud Examiners' (ACFE) 2024 Global Fraud Report, insider fraud contributed to over $3.1 billion in global losses, with organisations losing an estimated 5% of their annual revenue to fraud.[2] Recent Cifas data revealed a 14% rise in insider threat reported in 2023, with nearly half involving dishonest conduct by employees.

Alarmingly, 38% of those involved had been in post for less than a year, while 17% had held their positions for over a decade—showing that insider fraud can emerge at any stage of employment[3]. These threats now account for almost 30% of security breaches in the public sector, often involving misuse of sensitive data and manipulation of operational processes.[4]

Real-world cases underscore the damage insider fraud can cause. In 2024, Michael Paterson, a council tax team leader at Aberdeen City Council, was convicted of embezzling more than £1 million in public funds over a 17-year period. He manipulated his authority to process tax refunds, diverting hundreds of payments into his own accounts with no oversight.

The fraud persisted for nearly two decades due to critical control failures, including the absence of segregation of duties and passive enforcement of procedural safeguards. It was eventually uncovered when a colleague noticed an unusually large refund, prompting an internal review.

While Paterson did not reveal his motive, the longevity and sophistication of the scheme point to a calculated pursuit of personal gain, enabled by a perceived low risk of detection. The Accounts Commission described the case as a “cautionary tale” highlighting the dangers of relying on written controls without meaningful oversight or challenge.[5]

In 2024/25, a series of internal fraud cases within the Department for Work and Pensions (DWP) resulted in the loss of approximately £1.7 million in public funds. Investigations revealed that several civil servants exploited their access to benefit systems by manipulating identity verification procedures and approving claims without sufficient documentation or eligibility checks.

> Insider fraud presents a growing and often under-recognised threat within the UK public sector, where the stakes of trust, transparency, and public accountability are particularly high.

In one instance, a staff member authorised multiple fraudulent payments despite the absence of supporting evidence. These cases illustrate how access to sensitive systems, coupled with weak internal scrutiny, created clear opportunities for abuse. The lack of real-time oversight and reliance on trust over verification enabled individuals to bypass standard procedures for personal gain.

While formal motives were not disclosed, the nature of the fraud suggests a mix of opportunism and rationalisation. Some individuals may have been driven by financial pressures, while others likely viewed the system's weaknesses as a low-risk opportunity to exploit. The relatively modest scale of individual offences, combined with the volume of cases, points to a broader cultural problem where systemic gaps in monitoring and control created a permissive environment for misconduct.

Former pensions minister Baroness Altmann described the behaviour as “shocking” reinforcing the need for stronger enforcement, cultural change, and mechanisms that both deter fraud and detect it early.[6]

In a separate case concluded in May 2025, Dean Armitage, a ward manager at a mental health unit in Bradford, was sentenced to 18 months in prison for fraud by abuse of position.

Between April 2020 and October 2021, he falsified and backdated 185 overtime shifts, fraudulently claiming over £72,000 in salary and holiday pay. Armitage used his position to both author and approve these claims, circumventing basic verification procedures.

Although no motive was formally identified, the timing during the height of the COVID-19 pandemic suggests opportunism, potentially driven by burnout, entitlement, or financial strain. The case exposed weaknesses in oversight during crisis periods and demonstrated how short-term insider fraud can flourish in high-trust environments lacking active controls and routine scrutiny. These cases underscore how insider fraud within the public sector can take both sophisticated and opportunistic forms, highlighting the critical need for robust internal controls, credential checks, and proactive fraud detection mechanisms.[7]

Insider fraud is not a singular offence but a broad category encompassing asset misappropriation, financial reporting fraud, and corruption. These include theft of cash or physical assets, falsification of financial records, and abuse of power for personal gain through bribery, nepotism, or conflicts of interest. Despite their variety, such acts are unified by an insider's exploitation of their trusted role, often facilitated by gaps in internal controls or inadequate oversight.[8]
While weak controls are often the primary enabler, insider fraud ultimately stems from human behaviour.

Even with advances in technology and concerns about AI-facilitated misconduct, the root cause remains human—whether through prompting, programming, or collusion. To build meaningful defences, public bodies must design controls that address not only procedural gaps but also the psychological and behavioural dimensions of fraud. Academic literature identifies five key behavioural factors that influence insider fraud: motive, opportunity, rationalisation, integrity, and capability.[9] These form the basis of a behavioural risk lens that can strengthen control frameworks.

Motives are the personal drivers behind fraud, including financial need, greed, or non-financial triggers such as revenge, ego, or ideology. Opportunities arise when weak controls, poor oversight, or inadequate segregation of duties allow misconduct to go undetected. Rationalisation enables individuals to justify unethical actions—for instance, by claiming they are "borrowing" funds or "helping the organisation." Integrity refers to the moral character of individuals, and those with higher integrity are more likely to resist temptation.

Capability relates to the confidence, access, and skillset that allow certain individuals to commit fraud more effectively than others. This may include positional authority within the organisation, insider knowledge of accounting systems and control weaknesses, and a belief that they can evade detection or face minimal consequences even if exposed.[10]

To effectively reduce the motive to commit fraud, public bodies must address the human and emotional drivers that often underpin dishonest behaviour. While constrained pay is a reality in many parts of the public sector, transparency and fairness in pay structures can help minimise feelings of inequality or resentment. Equally important is ensuring fair access to promotion and career development.

When staff feel overlooked, undervalued, or perceive advancement to be based on favouritism rather than merit, frustration can build and, in some cases, be rationalised as justification for fraud.

Many instances of insider fraud are not motivated solely by financial gain, but by a sense of grievance or perceived injustice (e.g., where individuals feel mistreated, ignored, or disrespected) Treating employees fairly and with respect at every level through consistent management, transparent promotion processes, and serious handling of grievances helps reduce these revenge-based motives.

Involving staff in decisions that affect their roles and ensuring they feel heard can also prevent the kind of disengagement that fuels unethical behaviour. Providing access to employee assistance programmes, financial counselling, and mental health support can ease personal pressures that might otherwise lead to misconduct. Recognising ethical behaviour through praise, internal awards, or career development opportunities further reinforces a culture where integrity is both expected and rewarded. When staff feel respected, supported, and able to progress on merit, they are far less likely to justify fraud as a form of redress or survival. In this way, cultivating trust, fairness, and a sense of shared purpose becomes not only good organisational practice, but a powerful deterrent to fraud.

Reducing opportunities for fraud requires strong segregation of duties, even in small teams. Where staffing is limited, workarounds such as rotating responsibilities or peer reviews can serve as effective substitutes. Regular audits, including unannounced spot checks, and strict role-based access controls further limit the chances of fraud. The use of surveillance, data analytics tools, and fraud awareness training during onboarding and induction can enhance vigilance across the organisation. These measures should be supported by clear, well-communicated policies and procedures, particularly in high-risk areas such as finance, procurement, and recruitment, to eliminate ambiguity and close potential loopholes.

Monitoring and safeguarding physical and digital assets, including accurate inventory management and secure storage of sensitive records, are critical in preventing misuse or unauthorised access. Robust IT controls, including multi-factor authentication, system audit trails, and access reviews are essential, alongside regular data protection training to ensure staff understand their responsibilities in handling sensitive information.

Mandatory leave policies for employees in key roles can reveal suspicious activity during their absence, while exit procedures, such as prompt deactivation of accounts and review of recent activity help prevent last-minute misconduct by departing staff. Controls over system overrides, manual adjustments, and supplier relationships, like due diligence, conflict of interest declarations, and monitoring of payment patterns further reduce vulnerabilities.

Anonymous reporting channels empower staff to raise concerns early, even where direct oversight is limited. Crucially, fraud prevention must be underpinned by a clear framework of accountability, where consequences for fraud are consistently applied. This includes not only disciplinary action but, where appropriate, referral for criminal prosecution rather than quiet dismissal. Embedding fraud risks into organisational risk registers and ensuring senior oversight reinforces the message that fraud is a serious breach of public trust with real consequences.

> Controls must address not only procedural gaps but also the psychological and behavioural dimensions of fraud

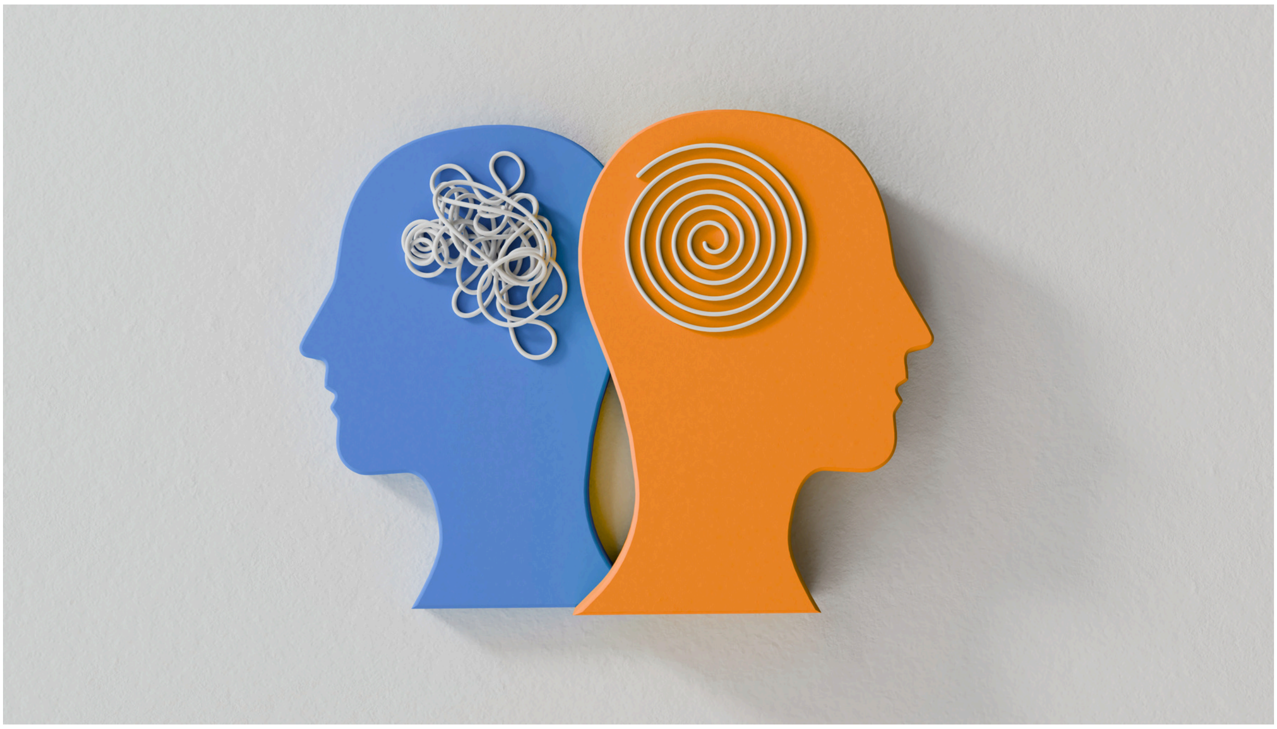
To challenge rationalisation, public bodies must embed a strong ethical culture as those with low integrity tend to rationalise their unethical behaviour. Codes of conduct should be regularly communicated and linked to real-world scenarios. Ethics training should go beyond legal compliance to include practical dilemmas in procurement or service delivery.

Consistent enforcement of ethical standards across all levels of staff reinforces accountability and discourages self-justifying behaviour. Promoting integrity starts with recruitment. Pre-employment checks and reference verification are essential, particularly for roles involving access to sensitive data or finances.

New employees should be asked to acknowledge the organisation’s code of conduct during onboarding, with regular reaffirmations. Ethical performance can be reflected in appraisals, and whistle-blower protections aligned with the Public Interest Disclosure Act must be visibly upheld to ensure concerns can be raised safely.

Managing capabilities involves limiting the power of individuals to override controls. Dual approval processes, audit trails, and regular reviews of system access are critical. Managers should be trained to recognise behavioural red flags and understand how control frameworks apply in practice. Regular audits should assess not only compliance, but also how well fraud prevention mechanisms are embedded into daily operations. Ultimately, insider fraud is rarely just a failure of process; it is often the result of psychological drivers such as resentment, rationalisation, entitlement, or perceived injustice. Effective prevention must therefore incorporate insights into why individuals choose to betray organisational trust.

By embedding behavioural risk into the design of fraud control frameworks considering not only what people can do, but why they do it, public bodies can build more targeted, realistic, and resilient defences. This human-centred approach strengthens accountability, supports ethical culture, safeguards public funds, and ultimately reinforces trust in the institutions that serve society.



Contact us:
Email: gcfp@cabinetoffice.gov.uk
Web: https://linktr.ee/CounterFraud