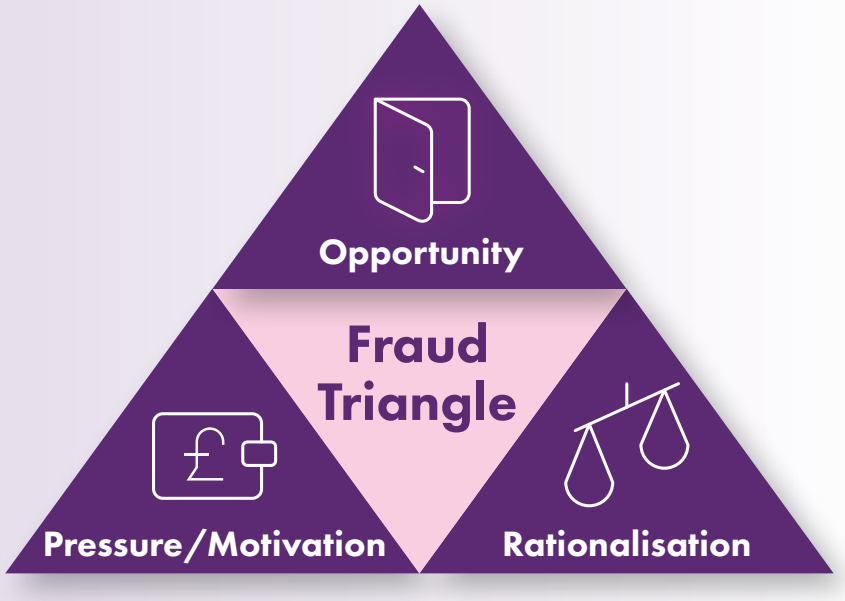
Northern Ireland Audit Office

Internal Fraud Risks



February 2022

Northern Ireland Audit Office

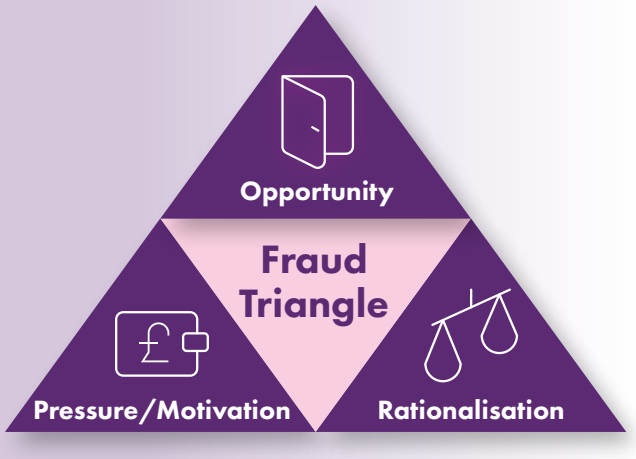
Internal Fraud Risks

Northern Ireland Audit Office
106 University Street
BELFAST
BT7 1EU

Tel: 028 9025 1000
email: info@niauditoffice.gov.uk
website: **www.niauditoffice.gov.uk**

What is internal fraud?

Internal fraud (also referred to as **staff fraud** or **insider fraud**) is fraud committed against an organisation by someone employed by that organisation. Internal fraud can range from minor thefts of assets or inflated expense claims up to major diversion of funds, accounting frauds or exploitation of payroll or client data. **A person employed** by an organisation includes contracted employees, temporary staff, agency workers and contractors.



Why does internal fraud happen?

Anyone in the organisation presents a potential fraud risk regardless of their position, age, gender or length of service.

Source: Managing the Risk of Fraud (NI): A guide for managers, Department of Finance, 2011

The **fraud triangle** is used by fraud experts to explain why fraud happens. When the three elements of **pressure, opportunity** and **rationalisation** combine, a person may cross the line into fraudulent behaviour. In addition, forensic fraud investigators refer to the **10-80-10 principle** whereby:

- 10 per cent of people will never commit fraud;
- 80 per cent of people may commit fraud when the three key elements coincide; and
- 10 per cent of people will actively seek to commit fraud.

So while the vast majority of people are honest and trustworthy, they also have the capacity to commit fraud, given a particular set of circumstances. The challenge for organisations is to minimise the risk of internal fraud by controlling the elements of pressure, opportunity and rationalisation as much as possible.

Opportunity is the most obvious area that organisations can influence, by having in place a sound system of internal controls which operates effectively. However, the actions of organisations can also influence **pressure** (for example, the expectation to meet challenging and unrealistic targets may cause an employee to commit internal fraud) and **rationalisation** (for example, an employee who considers themselves to have been unfairly treated by their employer may see that as justification for committing an internal fraud).

Internal Fraud

> ***Trusting but having the appropriate checks and balances in place is not the same as not trusting. It is basic management and governance.***
>
> **Source**: Public Sector Counter Fraud Journal, HMG, Issue 5, June 2020

Is internal fraud a risk for NI public sector organisations?

Internal fraud is a **real risk** within the NI public sector. Under Managing Public Money NI, all actual, suspected and attempted frauds affecting departments and their arm's length bodies must be reported to the Comptroller and Auditor General (C&AG). In the period from 1st January 2018 to 31st December 2021, 250 cases were notified to the C&AG where the perpetrator was internal to the organisation. Of these cases, 62 were reported as actual frauds. Examples of the types of frauds reported include:

- diversion of funds
- working elsewhere while off sick
- over-claiming expenses
- theft from a client.

Has COVID-19 increased the risk of internal fraud?

The COVID-19 pandemic has increased the risk of internal fraud in a number of ways, for example:

- Furlough may have led to staff shortages in some areas, compromising the application of internal controls.
- Changes in staff deployment may mean people are working in unfamiliar roles without a proper understanding of the procedures and controls which should operate.
- Working from home has now become the norm across many public sector organisations and this may have impacted on systems of internal control. Are controls still operating as they should in a remote working environment?
- Normal channels for staff or third parties to raise concerns about possible fraud risks may not have continued to operate effectively.
- The financial impact of COVID-19 on a household's income (e.g. due to furlough or redundancy) may mean staff are tempted to make up any shortfall through, for example, false claims for overtime or expenses, aware that normal controls may not be fully operating.
- The pressure to recruit additional staff in certain key areas, in a short timescale, may have led to increased recruitment fraud, e.g. use of fraudulent documentation to support applications.

How can organisational culture help minimise the risk of internal fraud?

Organisational culture is **fundamental** to minimising the risk of internal fraud. There needs to be a clear message from the top of every organisation that fraud will not be tolerated and will be dealt with effectively when it occurs. But senior managers and Board members must do more than send the right message, they must lead by example. They must behave in an **open, honest and ethical** way and make clear their expectation that all staff do the same. A positive culture is **everyone's responsibility**.

Organisational norms – the way things are done in a business – are an important influence on behaviour. The behaviour of others is an important cue – especially from senior leaders – and unethical behaviour can be contagious.

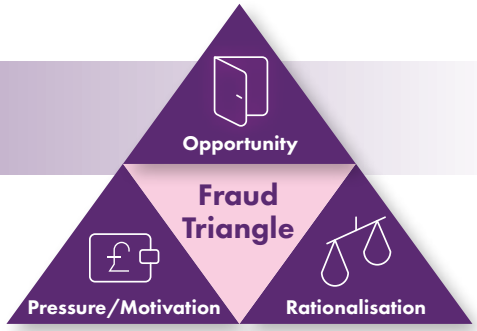
Source: Rotten apples, bad barrels and sticky situations: an evidence review of unethical workplace behaviour, CIPD, 2019

What are the consequences for an organisation if internal fraud risk is not addressed?

If an organisation does not effectively address internal fraud risk, there are a number of potential consequences, including:

- **financial loss** – the financial impact of internal fraud can be as significant as that of external fraud;
- **reputational damage** – internal fraud can significantly damage an organisation's reputation, perhaps more so in the public sector where public money is involved;
- **internal impact** – the impact within an organisation can be significant, for example by damaging trust and staff morale, and there will also be financial implications in terms of the cost of the investigation and disciplinary process and the recruitment process for a replacement staff member; and
- **regulatory implications** – organisations may face significant financial penalties if, for example, customer or client data is compromised.

Internal Fraud



Structure of the Guide

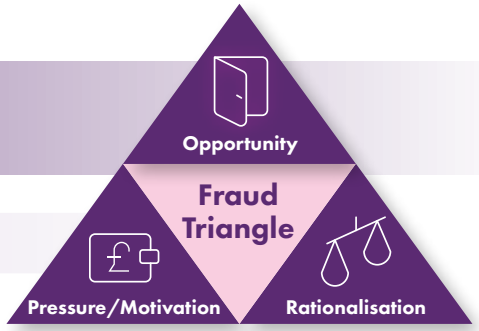
The Guide sets out the key fraud risks/red flags and mitigating controls under a number of headings:

- **General**
- **Employment application fraud**
- **Theft**
- **False claims**
- **Misuse of official assets**
- **Manipulation of official systems/processes**
- **Corruption**
- **Data/IT related fraud**

Further information

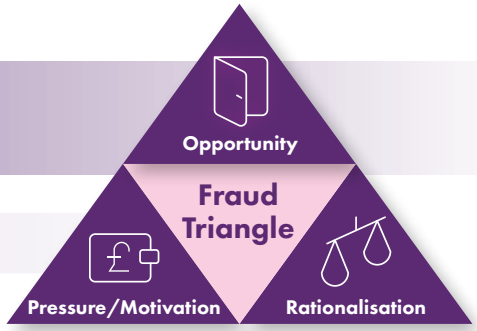
The Guide draws on information already in the public domain. You will find links to the **sources** used, illustrative **case examples** and a **self-assessment checklist** towards the end of the Guide. There is also a section on **internal fraud risk indicators** – the early warning signs of potential internal fraud.

General



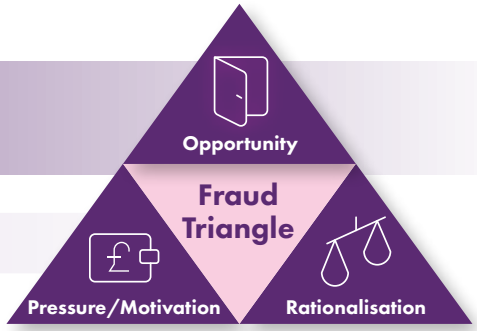
Fraud Risks / Red Flags	Mitigating Controls
• Your organisational culture may let minor misdemeanours and unethical behaviour go unchallenged.	✓ Senior managers and Board members must set the tone for the organisation by acting ethically and making it clear that all staff must do the same.
• There may be no clear responsibility for counter fraud arrangements at senior management level.	✓ A senior manager should be designated with lead responsibility for fraud prevention/counter fraud arrangements within the organisation.
• Middle managers/line managers may not recognise the importance of their role in influencing ethical behaviour and detecting the early signs of potential internal fraud.	✓ Effective line management supervision and support can help reduce the risk of internal fraud, by detecting and addressing any concerning behaviour in an employee. ✓ Line managers should maintain effective communication with their teams and provide constructive support and feedback. ✓ Line managers should tackle any issues of concern quickly so that employees do not become disgruntled.
• There may be no clear code of conduct or statement of ethical behaviour for the organisation.	✓ The ethical standards expected in an organisation must be made clear in the form of a code of conduct or equivalent. ✓ The code of conduct must be enforced actively, fairly and consistently if it is to be respected. ✓ The code of conduct must clearly define acceptable behaviour, e.g. in relation to gifts and hospitality and conflicts of interest, and be supported by relevant policies. ✓ The code of conduct must regularly be brought to the attention of staff. Ideally, staff should be required to sign up to the code annually.
• There may be no clear anti-fraud policy statement.	✓ Your organisation must have an anti-fraud policy in place which endorses a zero tolerance to fraud. ✓ The anti-fraud policy should be signed by the Chair/Chief Executive/Accounting Officer, to clearly demonstrate top level endorsement.
• There may be no understanding of the organisation's vulnerability to internal fraud.	✓ Your organisation should complete a fraud risk assessment, which should be reviewed and updated at least annually. It should include evaluation of internal fraud risks. For guidance, see 'Managing Fraud Risk in a Changing Environment', NIAO, 2015. ✓ Internal fraud risk factors to consider include: complexity of operations; adequacy of internal controls, such as separation of duties and supervision arrangements; nature and value of assets held; staffing arrangements etc. ✓ Internal fraud risks should be reassessed after significant events, such as changes in business processes and methods of working. The impact of remote working due to the COVID-19 pandemic is one example of this. ✓ Your organisation should be aware of internal fraud risk indicators at an organisational, operational and personal level (see Internal Fraud Risk Indicators section).

General



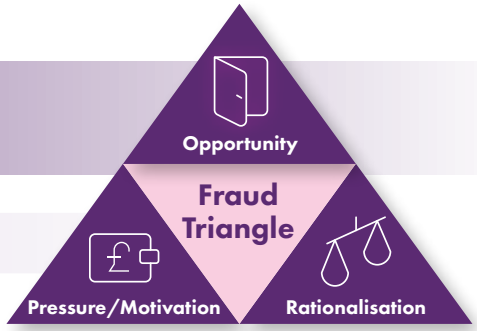
Fraud Risks / Red Flags	Mitigating Controls
• There may be a failure to recognise the importance of a sound system of internal controls, operating effectively.	✓ A sound system of internal controls, proportionate to identified risks, should be recognised as a key defence against internal fraud and a means of protecting all staff. **Trust is not a control**. ✓ Internal control systems must be tested regularly to ensure they are operating as intended. Internal control failures can make it more difficult to pursue successful criminal proceedings against an internal fraudster.
• Your organisation may fail to report frauds appropriately, both internally and externally, thereby reducing the opportunity to deter further fraud and share lessons more widely.	✓ Where internal fraud has been investigated and has resulted in disciplinary action, this should be publicised internally, for example on the staff intranet, to provide a deterrent effect. Care should be taken not to identify the individual involved. ✓ Under Managing Public Money Northern Ireland (Annex 4.7), all departments must report immediately to the Comptroller and Auditor General (C&AG) and the Department of Finance any actual, attempted or suspected frauds affecting them, their agencies and non-departmental public bodies. ✓ The Local Government Auditor (LGA) agreed with local councils that, from 1 April 2016, they should submit returns to the LGA about all actual, suspected and attempted frauds involving public money.
• There may be no clear and trusted route for staff to raise concerns about internal fraud.	✓ There should be a clear policy and procedures for staff wishing to raise concerns about possible fraudulent or unethical behaviour. The policy should be endorsed by senior management and the Board. ✓ A choice of reporting routes should be made available, e.g. via line management or a reporting hotline. Confidentiality should be assured. ✓ Arrangements for raising concerns should be regularly publicised and promoted within the organisation, e.g. via awareness training, staff intranet etc. ✓ Staff should be supported and encouraged to speak up and concerns received must be listened to and acted upon appropriately. ✓ Appropriate feedback should be given to those raising concerns about possible internal fraud, to demonstrate that the concern has been properly considered. ✓ The value of raising concerns should be demonstrated by publicising internally how concerns have been effectively dealt with. ✓ Organisations must be aware of current good practice in relation to raising concerns and how concerns should be dealt with. For guidance, see 'Raising Concerns: A good practice guide for the NI Public Sector', NIAO, 2020.

General



Fraud Risks / Red Flags	Mitigating Controls
• There may be no regular fraud awareness training/communications.	✓ There should be regular fraud awareness training for all staff (both at induction and on an ongoing basis). It should highlight the organisation's anti-fraud policy, code of conduct, fraud risk indicators, how to raise concerns etc. ✓ Your organisation should consider targeted fraud awareness training for staff in higher risk posts, e.g. finance or procurement. ✓ A strong anti-fraud message should be regularly communicated throughout the organisation, e.g. via staff newsletters, posters etc., as a deterrent to potential internal fraudsters.
• There may be an ineffective response to internal frauds which are discovered.	✓ In order to send the right signal, organisations must respond effectively when internal fraud is discovered, through robust investigations and the pursuit of sanctions and redress. Arrangements should be clearly set out in a fraud response plan. ✓ Organisations should not just allow fraudulent or corrupt staff to resign in order to avoid investigation and sanctions. Internal frauds should be reported to the police in accordance with your organisation's fraud response plan. ✓ Cases of internal fraud which have been investigated and have resulted in disciplinary action should be publicised to staff, to demonstrate an effective response and provide a deterrent effect. Care should be taken to ensure that any publicised information does not directly or indirectly identify the individual concerned.
• Poor staff morale can increase the risk of internal fraud by reducing staff loyalty.	✓ A positive, supportive environment will enhance staff morale and loyalty, and minimise motivation and rationalisation for committing fraud. ✓ The threats to staff morale need to be recognised and addressed. They may include lack of transparency, lack of fairness, reduced job satisfaction, unrealistic targets, low levels of staff engagement and no sense of purpose. ✓ An important element of a supportive environment is the provision of a confidential staff support service. Without such support, employees may become disgruntled and susceptible to undue influence.
• The significant increase in remote working due to the COVID-19 pandemic may have increased the risk of internal fraud.	✓ Organisations should assess the increased risk of internal fraud as a result of large scale remote working, e.g. due to less direct supervision of staff, and consider how the increased risk might be mitigated. This might include, for example, line managers having regular scheduled contact with team members, and reinforcement of culture/internal control messages via the organisation's intranet.

Employment application fraud



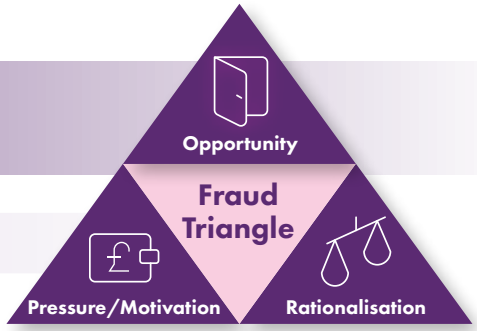
Fraud Risks / Red Flags

- A prospective employee may use a false identity.
- A prospective employee may use false documents in support of their application.
- A prospective employee may claim false qualifications in their application.
- A prospective employee may use false references.
- A prospective employee may conceal key information when applying for a job, such as an unspent conviction or unfavourable credit reference.

Mitigating Controls

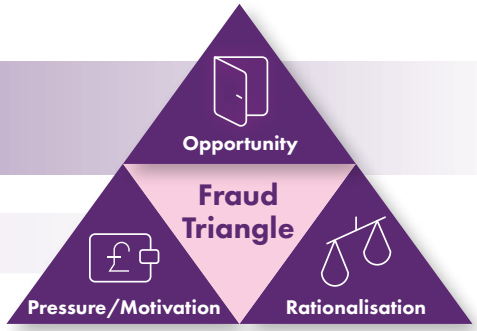
- ✓ Implement a sound system of pre-employment screening and due diligence, to ensure the applicant is who they say they are and to minimise the risk of fraudsters entering the organisation.
- ✓ Ensure your application form captures all the relevant information you will need for pre-employment screening, and includes a clear statement that pre-employment screening will take place.
- ✓ Ask prospective employees to sign a declaration that all information provided on their application is true and accurate, and point out that provision of false information will result in their application being withdrawn.
- ✓ Ensure the form includes the relevant "use of personal data" clauses to satisfy data protection legislation.
- ✓ The Baseline Personnel Security Standard is the minimum for government employees (identity, employment history, nationality and immigration status, and unspent convictions). In addition, all UK employers must ensure that prospective employees have the right to work in the UK.
- ✓ Consider additional checks such as academic/professional qualifications or a media search.
- ✓ Consider using targeted checks for specific higher risk posts, e.g. financial background checks for finance posts.
- ✓ Pre-employment checks should also be applied to temporary and contractor staff (e.g. cleaners and security staff).
- ✓ When employing staff via an agency, make sure there is clarity about who has responsibility for pre-employment checks (the agency or your organisation).
- ✓ Repeat screening should be considered for high risk or sensitive posts (as an employee's circumstances may change) or when a person moves to a higher risk post.
- ✓ If it becomes apparent that a prospective employee has included a material falsehood on their application, you should withdraw any job offer, notify the appropriate authorities, and notify the relevant recruitment agency if an agency worker is involved.

Theft



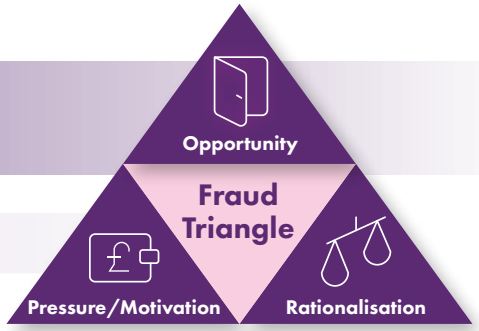
Fraud Risks / Red Flags	Mitigating Controls
• An employee may steal cash from their employer/colleagues/clients. • An employee may steal the personal property of colleagues/clients.	✓ Ensure fundamental controls are in place (see General section) - anti-fraud culture, code of conduct, robust internal controls etc. ✓ Ensure the recruitment process helps to prevent fraudsters entering the organisation (see Employment application fraud section). ✓ Ensure a clear separation of duties in high risk areas such as finance, to prevent diversion of funds. ✓ Be alive to the fraud risk indicators that may indicate an employee is likely to commit theft (see Internal Fraud Risk Indicators section) and, if necessary, increase supervision levels or move the person to lower risk duties. ✓ Ensure there is a clear and trusted route for employees to raise concerns about possible theft by colleagues.
• An employee may steal office equipment or fittings.	✓ Maintain up-to-date asset registers and ensure assets are clearly described. ✓ All assets and attractive items should be clearly marked as being the property of the organisation. ✓ Have a clear system for recording the issue and return of assets such as laptops, other portable devices, tools, equipment etc. ✓ Ensure that appropriate arrangements for the physical security of assets are in place. Carry out regular spot checks of assets.
• An employee may steal inventory items.	✓ Have robust inventory systems in place including comprehensive records, clear separation of duties and annual inventory checks by a person not involved in the inventory process.

False claims



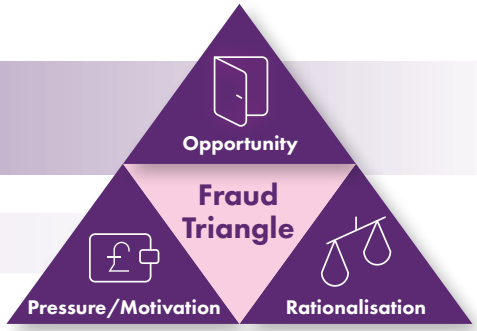
Fraud Risks / Red Flags	Mitigating Controls
• An employee may submit a false or inflated travel and subsistence claim. • An employee and supervisor may collude to secure expenses payments and split the proceeds.	✓ Ensure there is clear guidance on travel and subsistence and what can or cannot be claimed. ✓ Ensure there is a clear process of review and approval of claims by line managers. ✓ Countersigning officers should check claims against known work plans and standard mileages, and ensure that all necessary supporting documentation is provided (receipts etc.). ✓ Conflicts of interest must be declared (e.g. risk of supervisor authorising a claim from a spouse/partner/relative). For guidance, see 'Conflicts of Interest: a Good Practice Guide', NIAO, 2015. ✓ Consider the use of a counter fraud declaration on travel and subsistence claim forms ("I declare that the expenses I have claimed were incurred wholly, necessarily and exclusively in the execution of my duties as an employee. I confirm that I have personally incurred the expenditure and have not previously submitted any item on this claim"). ✓ Countersigned claims should be passed straight from the approving officer to the finance team for payment (and not via the claimant). ✓ The finance team should ensure correct rates are claimed, supporting documentation has been provided and the claim is properly authorised. ✓ Management should perform random sample checks to ensure controls are operating effectively. ✓ Management information and budget monitoring should be used to identify possible anomalies.
• An employee may submit a false or inflated overtime claim or timesheet. • An employee and supervisor may collude to secure overtime payments and split the proceeds.	✓ Ensure there are clear guidelines in relation to working hours, time recording/flexi time and overtime. ✓ Ensure there are clear reasons for any planned overtime and that it has been properly authorised by line managers before being worked. ✓ Authorising officers should consider claims for overtime in light of known workload/work plans, to determine reasonableness. ✓ Allocation of overtime should be on a fair and transparent basis in line with clear parameters. ✓ Conflicts of interest must be declared (e.g. risk of supervisor authorising a claim from a spouse/partner/relative) and properly managed. For guidance, see 'Conflicts of Interest: a Good Practice Guide', NIAO, 2015. ✓ Ensure appropriate monitoring and supervision of overtime work, to verify that employees are present and approved work is completed. ✓ Consider the use of a counter fraud declaration on overtime claim forms/timesheets. ("I declare that the information I have provided on this form is correct and complete. I understand that if I knowingly provide false information, this may result in disciplinary action and I may be liable for prosecution and civil recovery proceedings").

False claims



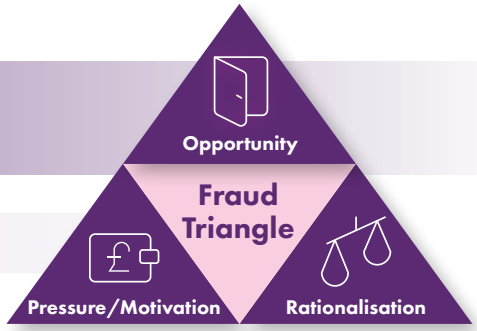
Fraud Risks / Red Flags	Mitigating Controls
	✓ Finance/HR should ensure that the correct overtime rate is applied and the claim is properly authorised, before processing for payment. ✓ Management should perform random sample checks to ensure controls are operating effectively. ✓ Management information and budget monitoring should be used to identify possible anomalies.
• An employee may claim to be off sick but is working elsewhere.	✓ Ensure there is clear guidance around secondary employment, including when a person is off on sick leave. ✓ Include in your code of conduct a requirement for employees to inform management about any secondary employment. ✓ Consider including a clause in contracts of employment which prohibits an employee from taking secondary employment without their employer's consent. ✓ Return to work interviews/forms should seek a declaration as to whether or not the person worked elsewhere while absent on sick leave.

Misuse of official assets



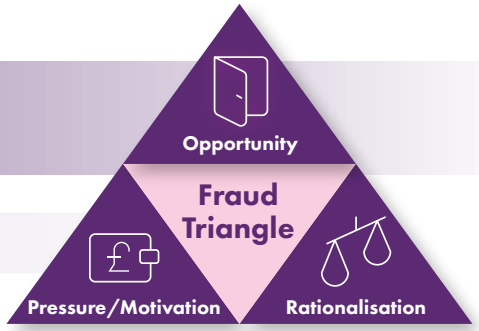
Fraud Risks / Red Flags	Mitigating Controls
• An employee may use official working hours and/or supplies and equipment to conduct personal business.	✓ Employees should be required to complete a declaration of any business interests or additional employment they may have, ideally on an annual basis and when circumstances change. ✓ Keep stock records up to date so that any anomalies around missing supplies are quickly identifiable. ✓ Ensure separation of duties between those ordering supplies, receiving supplies, and approving and paying invoices, so an employee cannot order items for their own benefit. ✓ Ensure there are clear arrangements around authorised signatories and authorisation limits for ordering supplies.
• An employee may use official tools/equipment/portable devices/transport for personal projects.	✓ Establish a system to record the issue and return of tools/equipment/portable devices. Undertake periodic reconciliations. ✓ Establish a system to monitor the use of official vehicles, through electronic tracking, mileage records, fuel usage etc. Query any anomalies.
• An employee may use an official procurement card for personal purchases.	✓ Establish a clear policy and rules on the use of procurement cards and communicate these to all staff. ✓ Make one person or central group responsible for issuing procurement cards and ensure the issue of cards is properly authorised. ✓ Maintain a record of cardholders and establish a monthly credit limit for each user. ✓ Ensure that cardholders submit claims regularly, supported by invoices and receipts, for payment processing and checking/reconciliation to card issuer statements. ✓ Ensure that cards are returned and destroyed when staff leave the organisation or cease to be cardholders.

Manipulation of official systems/processes



Fraud Risks / Red Flags	Mitigating Controls
• Internal controls in place may be insufficient to prevent/detect manipulation of systems /processes, or may not be operating effectively.	✓ Across the organisation, but particularly in high risk areas such as finance, payroll, HR and procurement, ensure that a sound system of internal controls is in place and is operating effectively, in particular: • separation of duties • rotation of staff • authorisation levels • supervisory checks • proper authorisation of changes to standing data.
• An employee in finance/accounts may manipulate the system to divert funds to a personal account. • An employee in finance/accounts may manipulate the accounting system to cover up a fraud. • An employee may submit false invoices to their employer which the employee is in a position to authorise for payment.	✓ Ensure separation of duties across the key elements of the financial process. ✓ Ensure proper authorisation of any changes or additions to payee details. ✓ Robust financial/governance controls should include transparent accounting records with full supporting documentation, and strong internal and external audit functions. ✓ There should be an audit trail of changes to key processes/transactions/ standing financial data, so that any anomalies can be followed up. ✓ Ensure payment reports are subject to supervisory checks before there is any transfer of funds. ✓ Implement a system of random management checks of accounting records, bank reconciliations etc. ✓ Monitor use of suspense accounts and journal entries to ensure there is a valid reason for them.
• An employee responsible for procurement/contracts/tendering may manipulate the process for personal gain, e.g. favouring the business of a family member or friend; purchasing items for personal use etc.	✓ Ensure separation of duties across the key elements of the procurement process. ✓ Ensure transparency around the criteria for tender evaluation, to minimise the risk of internal manipulation. ✓ Ensure tenders are held securely ahead of the evaluation process. Do not accept late tenders. ✓ Use standard tender templates or e-tendering to reduce the opportunity for internal manipulation. ✓ Ensure that any conflicts of interest are declared and properly managed, to avoid any perception of nepotism or favouritism. ✓ Ensure there are clear channels for suppliers and contractors to raise concerns about the tender process. Make sure that concerns are listened to and investigated appropriately. ✓ Implement a "No purchase order, no pay" policy, to ensure a full audit trail. ✓ Ensure that contract managers have had specific training around the risks of bribery/gifts/hospitality.

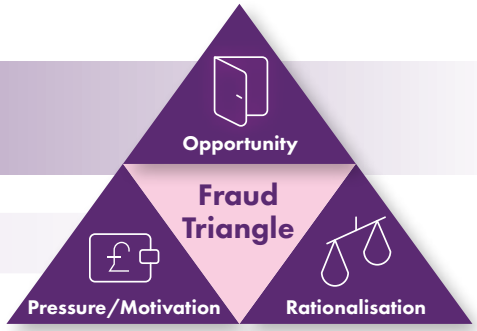
Manipulation of official systems/processes



Fraud Risks / Red Flags	Mitigating Controls
	✓ Ensure there are clear channels for staff to raise concerns about possible collusion, bribery and corruption. Make sure that concerns are listened to. ✓ Consider using data analytics to check supplier details against staff details (e.g. same address or bank account). This is one of the checks provided by the National Fraud Initiative (NFI), along with checking employee details to Companies House records. ✓ Ensure there are sound controls around changes to standing data such as supplier details. ✓ Always ensure approved delivery addresses are used and goods are not diverted to unexpected addresses. ✓ Confirm goods were properly ordered, authorised and received, before authorising payment. Only pay for goods ordered. ✓ For further detailed controls, see 'Procurement Fraud', NIAO, 2020.
• An employee in payroll/HR may manipulate the system to e.g. create a ghost employee or make an unauthorised amendment to pay/bonus rates.	✓ Run a report of starters/leavers/changes to standing data before each payroll run, for supervisory approval before being actioned. ✓ Produce regular exception reports for review by management. ✓ The payroll master file should be checked periodically by HR to ensure that the persons listed exist and that the correct salary and allowances are being applied.
• An employee in recruitment may manipulate the system to favour an applicant who is a family member or friend.	✓ Your organisation's code of conduct should make clear that nepotism and favouritism are not acceptable. ✓ Have a clear policy and procedures for recruitment which emphasise that decisions must be made objectively, based on the merits of the candidate. ✓ Recruitment panel members should be required to declare any connection to any candidate. If there is a connection, the panel member should be removed from the recruitment process. ✓ Ensure there are clear channels for staff to raise concerns about possible nepotism and favouritism. Make sure that concerns are listened to.

• An employee may manipulate internal systems/processes/records for their own or a third party's advantage, e.g. to:
  • remove or reduce a charge
  • influence the amount of grant payable to an organisation with which they are connected
  • influence a planning decision to the advantage of themselves/family member/friend.
	✓ Fundamental controls, as outlined above, must be in place and operating effectively, in particular:
	  • separation of duties
	  • rotation of staff
	  • authorisation levels
	  • supervisory checks.
	✓ Staff should be required to declare any interests which could be perceived to conflict with their official duties. Any such conflicts must be effectively managed.

Corruption



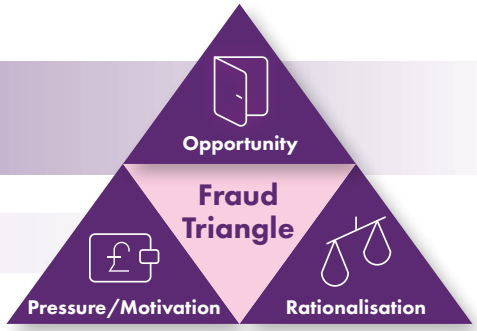
Fraud Risks / Red Flags

- An employee may be offered, or may request, a bribe to:
  - influence a tender/procurement process
  - influence a planning decision
  - provide a favourable inspection outcome
  - influence a decision to award a grant or licence.
- An employee may collude with contractors/suppliers in negotiating changes in price or specification.
- An employee may fail to declare an interest in a situation where they could use their professional position for personal gain (e.g. land holdings, shares).
- An employee may be subject to undue influence if they accept generous gifts, hospitality or other benefits.

Mitigating Controls

- ✓ There should be a clear commitment from senior management to prevent bribery and corruption, and a clear statement of ethical values.
- ✓ A proportionate bribery and corruption risk assessment should be carried out and reviewed periodically.
- ✓ A robust system of internal controls should be in place, including separation of duties, staff rotation and well-defined authorisation levels.
- ✓ There should be a comprehensive set of complementary policies, such as conflicts of interest, gifts and hospitality, anti-fraud and raising concerns.
- ✓ There must be a clear route for those wishing to raise concerns about actual or potential bribery and corruption.
- ✓ There should be arrangements in place for raising and reinforcing bribery and corruption awareness, as part of fraud awareness training or via staff bulletins on the intranet.

Data/IT related fraud



Fraud Risks / Red Flags	Mitigating Controls
• An employee may improperly access payroll/client data and pass it to third parties. • An employee may use payroll/client data to facilitate a fraud. • An employee may improperly view/amend the customer account of themselves, a relative or friend. • An employee may abuse IT/internet/email policies to commit fraud, e.g. false payment instructions.	✓ Ensure that a clear data/information/IT security policy is in place which includes defined roles and responsibilities, e.g. information risk owner. ✓ Promote a culture that values and protects data and recognises the importance of data security arrangements. ✓ Restrict access to sensitive data on a "need to know" basis. ✓ Ensure that access rights are regularly reviewed and amended/updated as appropriate, for example when someone changes role or leaves the organisation. ✓ Monitor the activities of those with rights to transfer personal or sensitive data, to ensure there is a continuing business need. ✓ Ensure arrangements are in place to log the activities of those processing data, providing an audit trail. Managers should periodically review any such logs to identify any suspicious activity. ✓ Regularly remind staff about the need for basic controls, such as locking their computer when left unattended and using strong passwords, to prevent interference/misuse by other staff members.
• The impact of COVID-19 and the significant rise in remote working has created a number of additional internal fraud risks, such as staff having access to sensitive data but without the usual level of supervision or the blurring of lines between work and personal environments, leading to lapses in data security.	✓ Ensure that your fraud risk assessment has been reviewed and updated for new IT/data related risks. ✓ Update systems, procedures and policies as appropriate, and reinforce messaging around, for example, use of personal devices. ✓ Monitor compliance with IT/data policies and be alert for red flags, such as employees sending work attachments to personal email addresses.
• An employee may be influenced to compromise your organisation's data, because of information posted on their social media accounts.	✓ Your code of conduct (see General section) should include provisions in relation to the proper use of social media, and cross-refer to the appropriate policy. ✓ Ensure you have a social media policy in place and that all staff are aware of its contents. The policy should direct staff not to post information about their employment on their social media accounts, as this may be used by fraudsters to influence the staff member.

Useful sources

Managing the Risk of Fraud (NI): a guide for managers, Department of Finance, December 2011

Fraud Risk Management: A guide to good practice, CIMA, 2012

Staff Fraud and Dishonesty: Managing and mitigating the risks, CIFAS/CIPD, June 2012

Ongoing Personnel Security: a good practice guide, CPNI, April 2014

Conflicts of Interest: a good practice guide, NIAO, March 2015

Payroll Fraud: guidance for prevention, detection and investigation, NHS, June 2015

Managing Fraud Risk in a Changing Environment, NIAO, November 2015

Managing the Risk of Bribery and Corruption, NIAO, November 2017

HMG Personnel Security Controls, Cabinet Office, May 2018

Rotten apples, bad barrels and sticky situations: an evidence review of unethical behaviour in the workplace, CIPD, April 2019

Raising Concerns: a good practice guide for the NI public sector, NIAO, June 2020

Procurement Fraud Risk Guide, NIAO, November 2020

Employment Screening: a good practice guide, CPNI, August 2021

Case examples

Case example – misuse of official assets:

An employee retained a fuel card for a temporary replacement council vehicle and then made fuel purchases for his own vehicle and for others, amounting to £4,000.

Following concerns that individual budget managers were not properly monitoring fuel card usage, the process was centralised. Centralised monitoring highlighted that purchases of unleaded fuel were being made on a card issued for a diesel vehicle, or for fleet vehicles not in use on the day of fuel purchase.

The employee was dismissed following a disciplinary process and was invoiced for the cost of the fuel fraudulently purchased with the card.

Source: *Review into the risks of fraud and corruption in local government procurement,* Ministry of Housing, Communities and Local Government (MHCLG), June 2020, Annex 4

Key lesson: Supervisory checks must be in place and operating effectively.

Case example – manipulation of official systems/processes:

A team leader in the Independent Living Service within a local authority purchased over £117,000 worth of items, which were not required by the service/clients, over a seven year period. Concerns were raised by a manager following a budget review. The fraud took advantage of a £300 threshold where orders did not require authorisation, and a particular arrangement with a retailer involving a trade card, where no order went to the supplier.

The concerned manager called in Internal Audit who reviewed the purchases and found items being purchased that were not consistent with the service. The purchases were being resold by the team leader on eBay. The member of staff received a 20-month jail sentence and confiscation order.

Source: *Review into the risks of fraud and corruption in local government procurement,* MHCLG, June 2020, Annex 4

Key lesson: Management information must be reviewed to detect possible discrepancies.

Case example – manipulation of official systems/processes:

An NHS training co-ordinator was concerned that his boss was hiring a friend to deliver training on suspicious terms which were costing the Trust over £20,000 a year. More courses were booked than were needed and the friend was still paid when a course was cancelled. The co-ordinator saw the friend enter the boss' office and leave an envelope. His suspicions aroused, he looked inside and saw that it contained a number of £20 notes.

The co-ordinator raised his concerns with a director at the Trust who called in NHS Counter Fraud. The suspicions were right: his boss and the trainer pleaded guilty to stealing £9,000 from the NHS and each received 12 month jail terms, suspended for two years.

Source: Protect (formerly Public Concern at Work)

Key lesson: There should be a clear route for staff to raise concerns about possible internal fraud; concerns should be dealt with effectively.

Case examples

Case example – theft and manipulation of official systems/processes:

A senior NHS manager stole over £800,000 from his employer over a seven-year period. He set up two companies and sent hundreds of fake invoices to the hospital trust in Essex. Individually, the invoices were all for relatively modest amounts, so the senior manager was authorised to sign them off without further checks. The senior manager had submitted a 'nil return' declaration of interests form to his employer.

The senior manager was jailed for two counts of fraud by cheating the Revenue and two counts of fraud by false representation, to serve five years and two months and two years concurrently.

The fraud was uncovered following a data matching exercise under the National Fraud Initiative (NFI), which compared employee details with Companies House records and trade creditor payments.

Source: Media reports, June 2021

Key lesson: Data analytics/data matching should be used to help detect possible internal fraud.

Case example – theft and manipulation of official systems/processes:

A manager in Land and Property Services (LPS) stole £189,000 over a 12-year period. He admitted two counts of fraud by abuse of position and six counts of fraud by false representation. The manager had extensive knowledge of the rates system and part of his middle management role involved processing rates refunds of up to £5,000, which occasionally occurred due to overpayments. He used his knowledge and position to circumvent controls by targeting older closed rate accounts with an outstanding credit balance, where the ratepayer could not be traced and therefore the refund could not be issued, and identified a system vulnerability that enabled him to amend the billing name and address and issue the refund to himself. He was also able to bypass the approval processes and system rules that needed to be satisfied before a refund could be paid. Another member of staff discovered suspicious activity on a rate account and raised concerns. An internal investigation examined over 2,000 refunds involving the manager and found that he had misappropriated over 50 of these, paying them to himself using various means, such as different addresses.

LPS has put in place additional controls to prevent a recurrence of this type of fraud. For example, billing details can now only be amended by staff who have no approval authority, thereby ensuring a separation of duties. More generally, LPS has thoroughly reviewed and strengthened its process checks, quality assurance reviews and monitoring of system access and functionality for users. The manager, described as a "trusted civil servant", was jailed for a year.

Source: Department of Finance and NI media reports, November 2021

Key lesson: 'Trust' must be supplemented by an effective system of internal controls.

Case examples

Case example – corruption:

Three NHS managers (two project managers employed via an agency and one in-house estates manager) defrauded a Welsh NHS body to the sum of over £822,000. One of the project manager's responsibilities included sourcing external contractors, approving tenders and quotes, authorising payments of invoices and verifying work completed. A works project was allocated £342,000 by the NHS body and the project manager directed that a specific contracting company be used. An investigation conducted by NHS Counter Fraud Services (CFS) Wales confirmed that the company was actually set up and run by the project manager, with the intention of paying himself for the work he was supposed to be contracting out on behalf of NHS body. In total, the project manager's company made over £822,000 from NHS contracts.

The project manager used the money to fund a lifestyle of luxury holidays, cars and property purchases. The second project manager knew from the outset that the first project manager was connected to the company, and the estates manager found out sometime later. Both became complicit in the fraud by accepting bribes in the form of envelopes containing cash or cheques, posted to their home addresses. The work that was actually carried out was done to a very poor standard, so the NHS body subsequently had to pay to have it corrected.

In November 2018, the three managers were sentenced to a combined total of 14 years in prison and were subject to confiscation orders.

Source: NHS CFS Wales, November 2018

Key lesson: Agency employees must be subject to the same due diligence and code of conduct requirements as direct employees.

Case example – theft and manipulation of official systems/processes:

In February 2005, the Sports Institute for Northern Ireland (SINI) appointed a Finance and Corporate Services Manager whose responsibilities included accountancy, payroll administration, banking, reconciliations and signing cheques. An office administrator discovered a series of suspicious financial transactions and raised concerns, resulting in an investigation. It found that the manager: had sole responsibility for bank transfers; dishonestly obtained the passwords to the on-line banking system, allowing him to create, authorise and execute payments to the bank accounts of his wife and daughter, disguising them as legitimate salary payments; hid the fraudulent payments in the bank reconciliations which he produced; and made changes to his PAYE records to dishonestly minimise his income tax. In total, the manager was estimated to have stolen over £75,000 in a 10-month period. He received an 18-month prison sentence, suspended for two years.

The investigation identified a number of control weaknesses which allowed the internal fraud to occur, including: a lack of separation of duties; outdated financial procedures; a lack of management supervision; and failings in corporate governance arrangements, in particular poor quality reporting to the Board and ineffective internal audit arrangements.

Source: *Internal Fraud in the Sports Institute for Northern Ireland,* NIAO, 19 November 2008

Key lesson: Fundamental controls, such as documented procedures, separation of duties and management supervision, must be in place and operating effectively.

Case examples

Case example – theft and manipulation of official systems/processes:

In August 2003, Ordnance Survey Northern Ireland (OSNI) uncovered an internal fraud which had been perpetrated over a five year period and resulted in a loss to OSNI of almost £71,000. The fraudster, who was a supervisor in Accounts Branch, replaced cash, which had been received from the sale of maps, with cheques to the equivalent value which he had stolen from incoming post. As credit controller, the fraudster created fictitious credit notes to amend customer accounts to the value of the stolen cheques, thereby clearing any outstanding debt. The fraud was discovered when the perpetrator went off on extended sick leave and was unable to cover his tracks.

The fraudster pleaded guilty to stealing cash and falsifying records and was sentenced to twelve months imprisonment, suspended for two years. He was also ordered to repay £30,000. The fraud persisted because of the absence of, or non-compliance with, basic controls. In addition, fraud indicators were missed, for example queries from customers whose accounts had been manipulated.

Source: *Internal Fraud in Ordnance Survey NI,* NIAO, 15 March 2007

Key lesson: Potential fraud indicators are early warning signs and must be followed up effectively.

Case example – theft

The chair of a Parents Teachers Association (PTA) defrauded the charity of over £35,000 over four years. The fraud was discovered following the appointment of new trustees who uncovered financial irregularities. They discovered that there were no financial controls in place, including no recording of money raised at fundraising events. Funds raised by the charity were also not forwarded to the school at regular intervals. A review of the PTA's financial records by the Trustees identified a number of failings. The matter was reported to the police who investigated the case.

The fraudster was convicted of five counts of theft and sentenced to two years in jail, suspended for two years, plus 300 hours of unpaid work. The PTA was able to recover £20,000 of the stolen money.

The PTA strengthened its internal controls by implementing formal cash handling procedures, bank signatories, monthly checking of bank statements by the PTA treasurer and regular submission of funds raised to the school.

Source: *Case studies of insider fraud in charities,* GOV.UK, April 2018

Key lesson: Basic internal financial controls are a fundamental requirement in any organisation, to help prevent internal fraud.

Case examples

Case example – false qualifications

A senior executive secured a series of high profile posts in the NHS on the basis of a number of false qualifications, including a degree and a Master of Business Administration (MBA). The deception came to light when, during a separate fraud case in which he was acquitted, his various job applications were assessed and there were found to be inconsistencies.

The fraudster admitted deception and fraud, and was jailed for two years. The court estimated that he had benefited by £643,000 as a result of his deception but assessed his available assets at only £97,737. Under the Proceeds of Crime Act 2002, he was ordered to pay this sum within three months, however this confiscation order was overturned on appeal.

Source: Media reports, 2018 and 2020

Key lesson: Effective pre-employment screening must be in place, in particular for senior posts.

Case example – false qualification

A senior manager in an Oxfordshire NHS Foundation Trust was found guilty of fraud after claiming in his job application that he had a degree, even though possessing a relevant degree was not an essential requirement for applicants; those with "at least ten years' experience in senior management positions within sizable organisations" could apply without one.

The fraud was discovered when all of the Trust's executive and non–executive directors' files were being updated in late 2017, as part of the Trust's duties under the 'fit and proper persons' checks. The manager was ordered by the court to complete 30 hours of rehabilitation and 200 hours of unpaid work.

Source: NHS Counter Fraud Authority, January 2020

Key lesson: Implement effective pre-employment screening to detect any fraudulent information provided by candidates.

Case examples – thefts in local councils

In the first case, an audit of a local council revealed that £12,000 cash income from market traders was unaccounted for. Internal control measures had failed. In particular, the audit found: a lack of income and budgetary control by senior managers; a single employee was involved in the collection and lodgement of cash; a lack of written procedures; and no countersigning of income returns. The council was able to offset some of the loss by way of monies due to the employee in question, and recovered the balance from his pension funds.

In a second case, poor internal controls over the purchase of goods for the canteen resulted in a loss of £3,600 to a council. The employee making the purchases, using petty cash, committed fraud by also purchasing items for personal use. The audit found a lack of regular monitoring of purchases and no documented procedures.

Source: Local Government Auditor reports, NIAO, June 2008 and June 2010

Key lesson: Basic controls such as documented procedures and effective supervision are essential, particularly where cash transactions are involved.

Self-assessment checklist

Please note: This checklist is **for guidance only** and is not intended to be exhaustive. It focuses on the **key good practice standards**, and should be considered in conjunction with the more detailed mitigating controls listed in the main sections of this Guide. It can be completed and reviewed/updated periodically to provide a degree of assurance in relation to your organisation's exposure to internal fraud risks.

Good practice standard	Yes / No	Action required
1. General		
1.1 Our organisation has a zero tolerance approach to fraud and corruption that is communicated to all staff in an anti-fraud policy, endorsed at a senior level. All staff are aware of their role in relation to fraud prevention.		
1.2 There is clear commitment from senior management and the Board that fraud will not be tolerated.		
1.3 We have designated a senior manager with lead responsibility for fraud prevention/counter fraud arrangements within our organisation.		
1.4 Our line managers are aware of their key role in reducing the risk of internal fraud through effectively supervising and supporting staff.		
1.5 We have a code of conduct which clearly defines acceptable behaviour for employees. All staff are required to sign up to this.		
1.6 There are arrangements in place for reporting and addressing conflicts of interest, including a register of interests. Staff are made aware of the need to declare potential conflicts of interest.		
1.7 Our organisation maintains a register of gifts and hospitality. Staff are aware of the need to register any gifts and hospitality received.		

Self-assessment checklist

Good practice standard	Yes / No	Action required
1.8 We have a fraud risk assessment in place which considers internal fraud risks and is reviewed and updated regularly. We are alive to the potential indicators of internal fraud.		
1.9 We have updated our fraud risk assessment in light of the increased risk of internal fraud due to the impact of COVID-19 on working arrangements.		
1.10 We have a sound system of internal controls in place, including separation of duties, staff rotation, effective supervision etc. Controls are regularly tested.		
1.11 We recognise that trust is not a control.		
1.12 Our organisation has an internal raising concerns policy and procedures in place. These are accessible to all staff and offer a choice of reporting routes.		
1.13 We encourage and support staff to raise concerns about possible internal fraud.		
1.14 All staff receive fraud awareness training, both at induction and on an ongoing basis. Targeted training is provided to staff in higher risk roles, such as finance and procurement.		
1.15 We respond effectively when an internal fraud is discovered, in accordance with our fraud response plan.		
1.16 We report appropriately on frauds internally, and report externally as required by Managing Public Money Northern Ireland or as advised by the Local Government Auditor.		

Self-assessment checklist

Good practice standard	Yes / No	Action required
1.17 We recognise the importance of good staff morale in minimising the risk of internal fraud, and seek to create a positive, supportive working environment.		
1.18 We recognise the negative impact that COVID-19 working arrangements may have had on staff morale and seek to mitigate this through regular team contact and reinforcement of culture/internal control messages.		
2. Employment application fraud		
2.1 We implement a sound system of pre-employment screening to minimise the risk of fraudsters entering our organisation. We recognise that the Baseline Personnel Security Standard is the minimum for government employees.		
2.2 We ask prospective employees to sign a declaration that all information provided on their application is true and accurate.		
2.3 We consider using targeted checks for specific higher risk posts.		
2.4 We ensure there is clarity about responsibility for pre-employment checks when employing agency staff.		
3. Theft		
3.1 We ensure separation of duties in high risk areas such as finance, to prevent diversion of funds.		

Self-assessment checklist

Good practice standard	Yes / No	Action required
3.2 We are mindful of the fraud risk indicators which could indicate theft by an employee.		
3.3 We maintain up-to-date asset registers and perform regular spot checks.		
3.4 We have robust inventory systems in place, including clear separation of duties.		
4. False claims		
4.1 We have clear guidance on what can be properly claimed regarding travel and subsistence, working hours and overtime.		
4.2 We have robust authorisation procedures in place. Potential conflicts of interest are properly managed.		
4.3 We use the appropriate counter fraud declaration on internal claim forms.		
4.4 We have clear rules around secondary employment.		

Self-assessment checklist

Good practice standard	Yes / No	Action required
5. Misuse of official assets		
5.1 We require employees to declare any business interests or additional employment they may have.		
5.2 We ensure separation of duties in relation to supplies.		
5.3 We have effective systems for monitoring the use of official assets.		
5.4 We tightly control the issue and use of procurement cards and reconcile expenditure to card issuer statements.		
6. Manipulation of official systems/processes		
6.1 We have fundamental internal controls in place, including separation of duties, rotation of staff, supervisory checks and proper authorisation of changes to standing data.		
6.2 We recognise the importance of complete documentation and a full audit trail.		
6.3 We ensure that conflicts of interest are declared and properly managed, to avoid any perception of nepotism or favouritism.		
6.4 We make proactive use of management information and data analytics to detect anomalies and inconsistencies, which could indicate internal fraud.		

Self-assessment checklist

Good practice standard	Yes / No	Action required
7. Corruption		
7.1 We have a clear statement of ethical values for our organisation and consider bribery and corruption risks as part of our fraud risk assessment.		
7.2 We have comprehensive policies covering conflicts of interest and gifts and hospitality, to avoid any uncertainty as to what is acceptable.		
7.3 We raise awareness of bribery and corruption risks as part of fraud awareness training for all staff.		
8. Data/IT related fraud		
8.1 We have a comprehensive data/IT policy in place which includes defined roles and responsibilities.		
8.2 We ensure that staff access rights to sensitive data/IT systems are regularly reviewed, and updated/amended as appropriate.		
8.3 We ensure there is a full audit trail in relation to data being processed, which is periodically reviewed by management to identify any suspicious activity.		
8.4 We have reassessed internal data/IT fraud risks in light of revised working arrangements due to the COVID-19 pandemic.		
8.5 We have a social media policy in place which highlights the risks of staff posting information about their employment online, thereby leaving them open to possible undue influence by fraudsters.		

Internal Fraud Risk Indicators

Organisational Indicators	Operational Indicators	Personal Indicators
• Lack of effective Board/Audit Committee oversight • No fraud risk assessment • Lack of anti-fraud policy and fraud response plan • Lack of clear financial delegations • Climate of fear or an unhealthy corporate culture • Lack of established code of ethical conduct • Lack of thorough investigation of alleged wrongdoings • Strained relationships between management and internal/ external auditors	• Inadequate recruitment processes and staff screening • Lack of segregation of duties/rotation of staff • Lack of management supervision of staff • Excessive staff turnover in key control areas • Dissatisfied staff in key control areas • Significant workforce reductions/redundancies • Inadequate testing of internal controls • Absence of key controls and audit trails • Management frequently overriding internal controls • Consistent failure to correct control weaknesses • Missing or unavailable official records • Photocopied/altered documentation • "Rubber stamp" or missing authorisation signatures • Bank reconciliations not maintained or not balanced • Extensive use of suspense accounts and journal entries • Unauthorised changes to systems or work practices • Excessive control of all records by one officer • Suppliers/contractors who insist on dealing with one particular member of staff • Multiple cash collection points/remote locations • Poor physical security of assets • Differences between inventory and stock records • Poor access controls to IT systems • Poor IT security practices/breaches in data security • Systems being accessed outside normal working hours • Control/audit logs being switched off	• Employees apparently living beyond their means • Employees with outside business interests or other jobs • Employees with drink, drug or gambling problems • Employees suffering financial hardships, e.g. borrowing from fellow employees • Employees who are first to arrive in the morning and last to leave at night • Egotistical employees (e.g. scornful of system controls) • Marked character changes in employees • Employee secretiveness • Employees working unusual hours on a regular basis • Employees who refuse to comply with normal rules and practices • Employees not taking leave, or working excessive overtime • Employees socialising with contractors or suppliers, accepting meals, drinks or holidays • Disgruntled employees

Published by CDS

CDS 266635