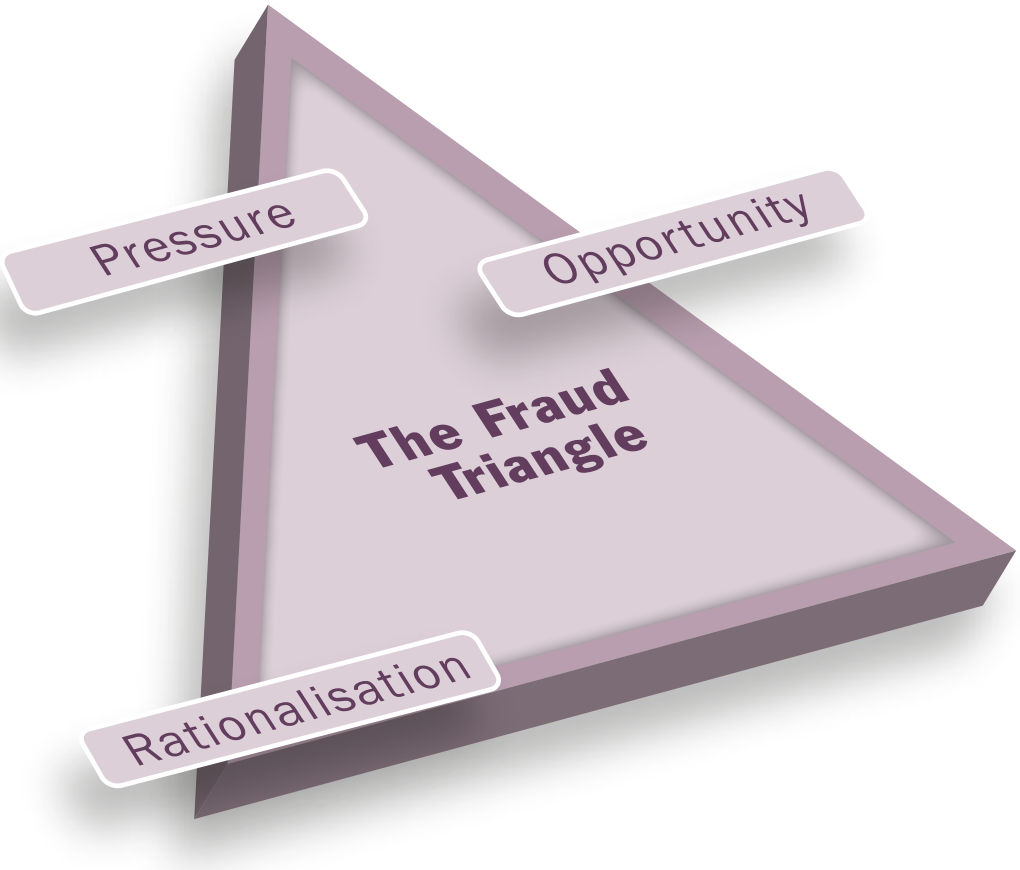
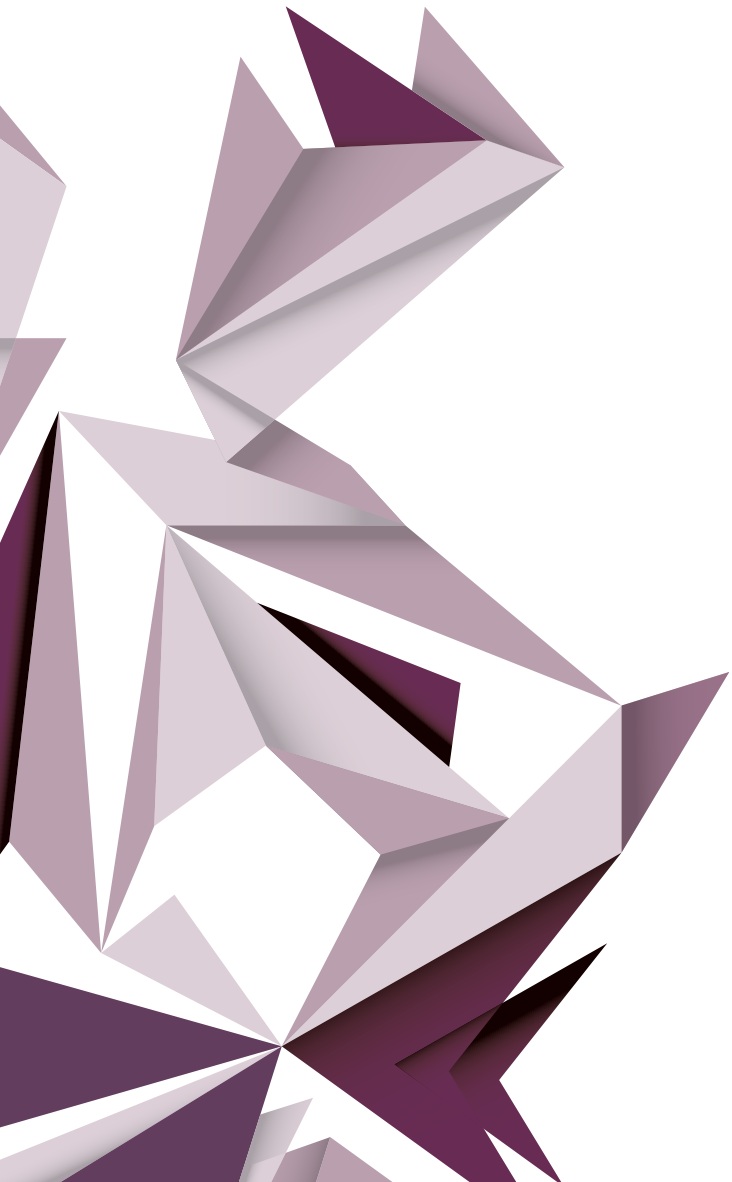
NIAO

Northern Ireland Audit Office

Managing Fraud Risk in a Changing Environment

A Good Practice Guide



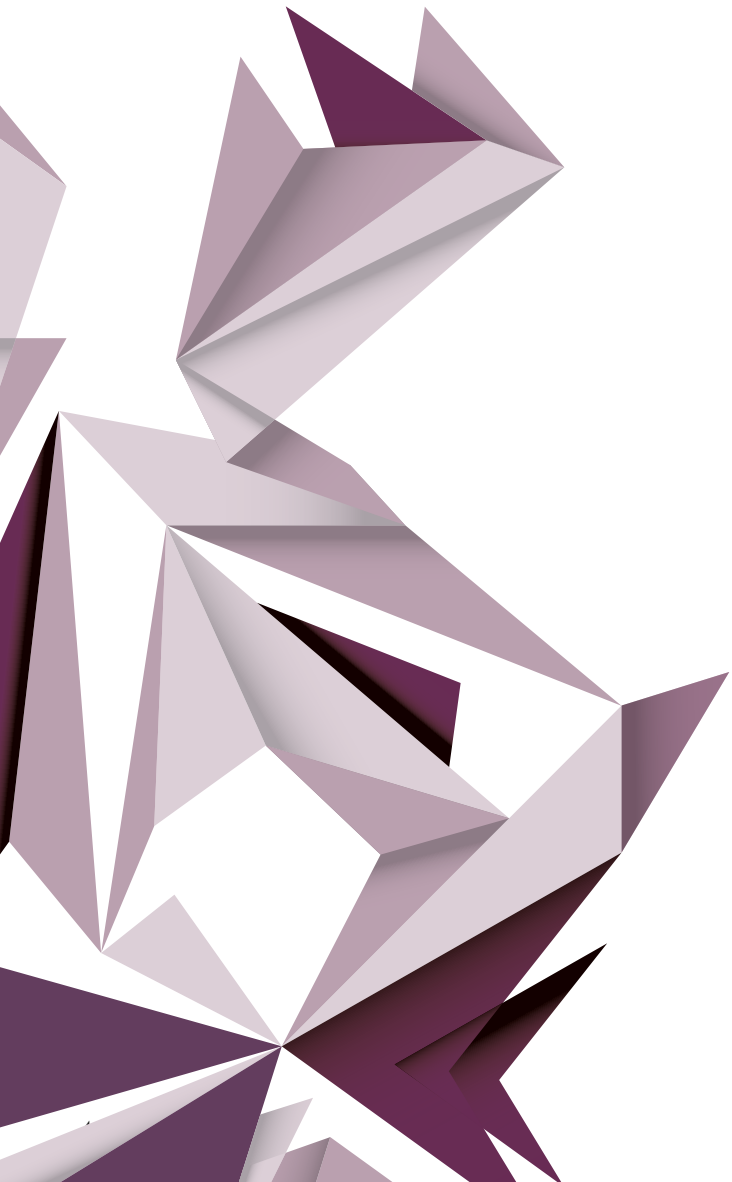


Northern Ireland Audit Office

Managing Fraud Risk in a Changing Environment A Good Practice Guide

Published 17 November 2015

Contents



Introduction

Organisational change is an essential feature of the public sector as it seeks to improve and become more efficient. Nevertheless, it is a widely accepted principle that the risk of fraud escalates in periods of significant change. The Northern Ireland (NI) public sector is currently in the middle of a period of unprecedented change on a number of fronts:

- From 1 April 2015, the number of local councils reduced from 26 to 11 under local government reform.
- From 1 April 2015, a single Education Authority replaced the five education and library boards and the Staff Commission for Education and Library Boards.
- During 2016, the number of Northern Ireland government departments is planned to reduce from 12 to 9, with significant reallocation of responsibilities. This has been described as the most extensive reorganisation of departments since 1999, with changes being made within a "pressing timescale".[1]
- Continuing budgetary pressures have led to significant staff reductions across the public sector, achieved mainly through a voluntary exit scheme. The NI Finance Minister has described the scope and speed of the exit scheme as unprecedented in the history of the NI civil service.
- Budgetary pressures mean there is an on-going need to achieve efficiencies in service delivery.

As new public sector organisations are created, or formed through a process of merger, a number of key fraud risks may emerge, for example:

- roles and responsibilities may be unclear or inadequately defined;
- governance arrangements may not operate effectively;
- staff reductions may lead to weakened control systems due to inadequate segregation of duties;
- staff losses on a significant scale may mean that key skills are lost; and
- supervisory checks may be overlooked.

Losses to fraud in the public sector are estimated at three pence in every pound spent.[2] With annual public expenditure of around £20 billion in Northern Ireland, this means that potentially £600million could be lost to fraud. This is money that cannot be spent on frontline services. At a time of austerity, fraud is a key risk and it is essential that losses to fraud are minimised as far as possible. It is also widely recognised that in times of financial constraint, people are more likely to commit fraud.

1 OFMDFM Oral Statement to the NI Assembly, 2nd March 2015

2 *Eliminating Public Sector Fraud*, Cabinet Office and National Audit Office, June 2011

This Guide highlights the reasons why fraud can occur, the key risks that may emerge in times of significant change and the policies, procedures and controls that should be in place to address those risks. It draws on documents already in the public domain and uses the key principles from those documents to reinforce the need for increased fraud awareness in this dramatically changing environment.

The Guide provides an initial high level aide memoire for new and merged organisations dealing with fraud risk in a changing environment (see page 3). It also includes detailed self-assessment checklists at the end of each section, to help organisations measure how well they are preventing, detecting and responding to fraud.

Fraud risk in a new or merged organisation - aide memoire

This checklist should be used as an initial high level aide memoire for new and merged organisations, in conjunction with the detailed checklists provided at the end of each section of this Guide.

☑ ☒

- ☐ Has our organisation included counter fraud arrangements in the change management process, so they are not overlooked?
- ☐ Have we allocated clear responsibility to a designated senior manager for overseeing the establishment of a counter fraud strategy in the new/merged organisation?
- ☐ Does that designated manager have access to, and the full support of, the Audit Committee?
- ☐ Have we secured counter fraud expertise to provide guidance on fraud-proofing any new systems and processes?
- ☐ Have we fully considered the impact of significant staff reductions on our internal control environment? Controls may need to be reprioritised to ensure that key fraud risks continue to be addressed.
- ☐ Have we considered, as a priority, the fraud risks associated with a period of change and the mitigating controls highlighted in Figure 8 of this Guide?
- ☐ Have clear channels been established for staff to raise concerns during the transition period?
- ☐ Have any changes to established whistleblowing arrangements and points of contact been made clear and communicated to all staff?

Why does fraud occur?

The right conditions for fraud

The majority of people have the propensity to commit fraud if the conditions are right. 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 if certain key factors coincide; and
- 10 per cent of people will actively seek to commit fraud.

The key factors which generally coincide when fraud occurs are **Pressure**, **Opportunity** and **Rationalisation**, commonly known as the **Fraud Triangle**.

The Fraud Triangle

The concept of the Fraud Triangle was developed in the 1950s by criminologist Dr. Donald Cressey, following a study of 200 convicted fraudsters and their motivation for committing the crime.

Pressure:

Motivation or incentive to commit fraud

Opportunity:

Ability to carry out fraud

Rationalisation:

Justification of dishonest actions

Pressure

Pressure or motivation to commit fraud can come from a range of sources. Examples include:

- a tight economic climate, with minimal pay rises and the threat of job losses;
- pressure to maintain the same level of performance with fewer resources; and
- having to meet what are perceived as unrealistic targets.

The 10-80-10 principle suggests that, while most people are fundamentally honest, they may succumb to such pressures if the opportunity arises.

Opportunity

Opportunity to commit fraud generally arises as a result of system control weaknesses. Control weaknesses can occur for a variety of reasons, for example:

- downsizing can mean there are fewer people to facilitate effective separation of duties, a key component of internal control;
- restructuring can affect the control framework of an organisation by removing some key checks and balances; and
- a lack of clear roles and responsibilities in new or merged organisations can mean that management supervision is ineffective.

Significant change can therefore provide greater opportunity for fraud.

Rationalisation

Rationalisation is the third element of the fraud triangle necessary to make a person who would not normally commit a crime step over the line into criminality. Times of economic pressure can increase a person's capacity to justify their fraudulent actions. An initial act of taking money may be regarded as a "loan" that the person intends to repay but if the act goes undetected due to control weaknesses, the person may be tempted to repeat the act and so the fraud grows. Justification for fraud may be that "others are doing it", or low staff morale caused by job cuts, pay freezes and budgetary pressures may lead someone to think that their employer "owes" them.

The "Perfect Storm"

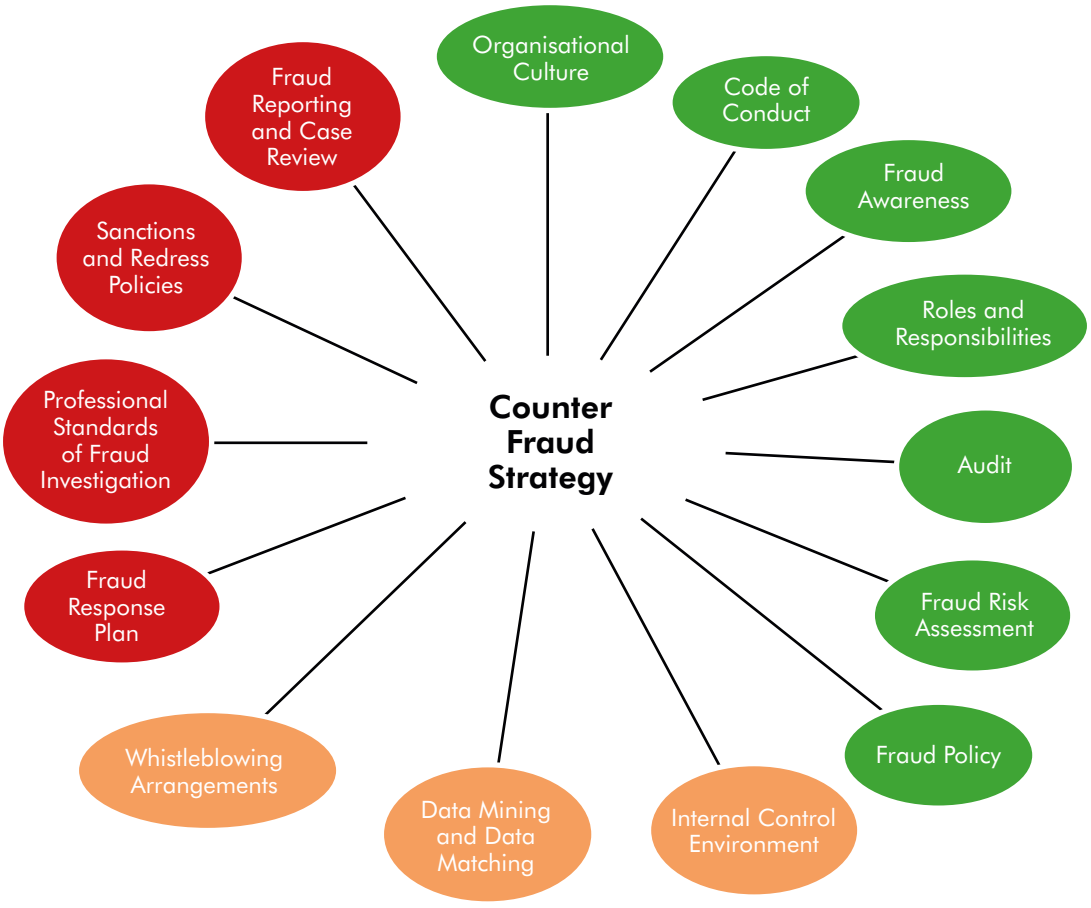
Many writers refer to the "perfect storm" when the three elements leading to fraud coincide. The unprecedented changes across the NI public sector provide ideal conditions for this "perfect storm" and underline the need for awareness of an increased fraud risk in a dynamic environment, and a clear strategy for dealing with the increased risk.

Addressing fraud risk

A key requirement in addressing fraud risk is a **counter fraud strategy**. CIPFA's Code of Practice[3] on managing fraud risk states: *"An organisation needs a counter fraud strategy setting out its approach to managing its risks and defining responsibilities for action."*

A counter fraud strategy comprises a number of complementary elements, as illustrated in Figure 1 (this list is not exhaustive).

Figure 1: Counter Fraud Strategy



The elements of the strategy are designed to:

- **prevent fraud;**
- **detect fraud;** and
- **respond to fraud** when it occurs.

3 *Code of Practice on managing the risk of fraud and corruption*, CIPFA, January 2015

Preventing fraud

The best way to minimise fraud losses is to stop fraud happening in the first place. Key fraud prevention measures may be:

- cultural;
- organisational;
- operational.

Preventing Fraud – Cultural Measures

Cultural factors, as outlined in Figure 2, can play an important part in minimising fraud risk within an organisation.

Figure 2: Preventing Fraud - Cultural Measures

Culture

The Board and senior management are responsible for setting the right tone across an organisation, with a clear endorsement of **ethical values** and a **zero tolerance to fraud**. In a newly formed or merged organisation, it is essential that the new Board makes a clear statement as early as possible that fraud will not be tolerated, and leads by example. CIPFA's Code of Practice on managing fraud risk states *"The governing body should acknowledge its responsibility for ensuring that the risks associated with fraud and corruption are managed effectively across all parts of the organisation."*

Code of Conduct

A code of conduct is one of the most important means of defining the **standards expected** of all employees. Newly formed public sector organisations must ensure that a code of conduct is put in place as soon as possible. The code should set out the standards expected in the professional and personal lives of employees, highlight the risk of conflicts of interest and establish boundaries in terms of gifts and hospitality. The code should also make clear that staff are expected to report fraud by colleagues, contractors and suppliers when they become aware of it. Staff in new and merged organisations should be required to sign up to their code of conduct annually and declare any conflicts of interest.

Fraud Awareness

All staff have a role to play in preventing fraud. They must be made aware of their role and reminded of it on a regular basis. As the opportunity for fraud increases during times of significant organisational change, it is essential that fraud awareness is given a high profile in new public sector organisations. Fraud awareness can be raised in a variety of ways – for example, training programmes, fraud and whistleblowing policies, use of intranet and staff bulletins and tailored training for staff in high risk areas.

Sources: *Managing the Risk of Fraud: A Guide for Managers*, Department of Finance and Personnel, December 2011
Fraud Risk Management: Developing a Strategy for Detection, Prevention and Response, KPMG, 2006
Code of Practice on managing the risk of fraud and corruption, CIPFA, January 2015

Preventing Fraud – Organisational Measures

A sound anti-fraud culture must be complemented by organisational structures which enhance that culture. Key organisational factors include:

- clear roles and responsibilities; and
- a strong audit committee and audit function (e.g. internal audit and external audit).

How does significant change impact on roles and responsibilities?

Addressing fraud risk in an organisation is a management responsibility but staff at all levels have a role to play. Established organisations should have stable staffing structures with clear designation of responsibilities and clear lines of accountability. Stability helps underpin the hierarchical roles and responsibilities outlined at Figure 3. However, in a period of significant change there is a risk that staffing structures become unstable and lines of accountability blurred.

Figure 3: Roles and responsibilities for addressing fraud risk

- **Accounting Officer/Chief Executive:** Overall responsibility for fraud risk management must sit at the head of an organisation. This is often referred to as the "**tone from the top**" and the head of any public sector organisation must send out a very clear message that fraud in any shape or form, committed against the organisation by anyone internally or externally, will not be tolerated and will be dealt with in the strongest possible way.
- **Senior officers:** Operationally, there should be a **designated senior manager** responsible for ensuring that fraud risk is addressed across the organisation in a structured way. Ideally, this designated person should attend Board meetings and have delegated authority for decision making in relation to fraud risk management. They should be supported by the team of senior managers responsible for individual business areas within the organisation. In this way, responsibility for fraud risk can be apportioned but a central focus will always be maintained.
- **Line managers:** Line managers at all levels should be responsible for **ensuring that systems and processes** are put in place to reduce fraud risk (the "control environment") and **are operating as they should**. Line managers should be answerable to the senior manager for their business area in relation to fraud risk.
- **All staff:** Fraud is committed by individuals so it is **up to each individual to act in an ethical way** and in accordance with principles and guidelines which seek to minimize the risk of fraud. All public servants should be mindful of the Seven Principles of Public Life (the Nolan principles) and the requirements of their organisation's code of conduct.
- **Counter fraud staff:** **Counter fraud specialists**, either within the organisation or as external advisors, can also have a **key role** in advising senior management on fraud prevention and detection measures.

Sources: *Code of Practice on Managing the Risk of Fraud and Corruption*, CIPFA, December 2014
Managing the Risk of Fraud (NI): A Guide for Managers, Department of Finance and Personnel, December 2011

The Role of Audit

Internal audit staff are not responsible for preventing or detecting fraud[4] but can provide expert advice to senior management within an organisation in relation to the controls which should be in place to minimise fraud risk. The role of **external audit** is primarily to give an opinion on whether the financial statements of an organisation are true and fair and expenditure and income has been applied to the intended purposes. In doing so, external auditors will need assurance that the financial statements are free from material levels of fraud or error.

4 *Fraud and the Government Internal Auditor*, HM Treasury, January 2012

So while they have an interest in fraud risk, **auditors do not have direct responsibility for preventing or detecting fraud**.

The Audit and Risk Assurance Committee[5]

The Audit Committee in any organisation plays a key role in reviewing the risk management and control environment of that organisation. This includes fraud risk and the system of controls put in place to mitigate fraud risk. Figure 4 highlights the key functions of an Audit Committee.

Figure 4: The Audit Committee role

To fulfill its role effectively, the Audit Committee must:

- understand the organisation's business strategy, control environment and risks, including fraud risk;
- understand the role of those charged with governance in relation to managing risk, including fraud risk;
- be familiar with the organisation's policies and procedures relating to fraud risk;
- understand the organisation's framework and allocation of responsibilities for risk management;
- be aware of the vulnerability of the organisation to changing conditions, such as economic pressures;
- critically review and challenge the framework for managing risk, including fraud risk; and
- critically review and challenge the control environment in place to mitigate risk, including fraud risk.

Sources *Audit and Risk Assurance Committee Handbook (NI)*, Department of Finance and Personnel, March 2014
Managing Fraud Risk: The Audit Committee Perspective, Grant Thornton

The role of the Audit Committee in addressing fraud risk is therefore to support management through a process of challenge and review from a position of knowledge, and provide advice as appropriate.

Audit and Assurance in New Organisations

As new public sector organisations are created through merger or the transfer of responsibilities, it is essential that audit staff and audit committees provide meaningful assurance and challenge functions during the transition period and beyond. The current changes across the NI public sector are likely to lead to the reorganisation of the internal audit function but it is essential that the value of its role is not diluted.

The following **case example** illustrates how fraud occured when a member of staff acted unethically and the audit function was ineffective.

5 This may more commonly be known as the Audit Committee.

Case Example - Sports Institute for Northern Ireland (SINI)

In February 2005, SINI appointed a Finance and Corporate Services Manager whose responsibilities included accountancy, payroll administration, banking, reconciliations and signing cheques. A series of suspicious financial transactions discovered by an office administrator alerted SINI, and an investigation was launched. It found that the fraudster:

- had sole responsibility for bank transfers and used the Bankers' Automated Clearing System (BACS) facility to make payments;
- 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. In his role as payroll administrator he was able to disguise these payments as legitimate salary payments to other members of SINI staff and as contributions to the pension fund. These payments were, in fact, being made by cheque;
- hid the fraudulent payments in the bank reconciliations which he produced;
- made changes to his PAYE records to dishonestly minimise his income tax; and
- drew funds from the SINI bank account using a number of cheques, payable to cash.

In total, the Sports Council estimated that he stole £75,041 in a period from October 2005 to August 2006.

The investigation identified a number of control weaknesses which allowed the fraud to occur, including:

- a lack of separation of duties;
- a financial procedures manual which was outdated and not adhered to;
- a lack of management supervision; and
- failings in corporate governance arrangements, in particular
  - » poor quality and inconsistent reporting to the Board; and
  - » ineffective internal audit arrangements, whereby the auditors reported to the fraudster and not to the Board and were obstructed in their work by the fraudster.

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

Preventing Fraud – Operational Measures

To help prevent fraud, it is important that organisations have a clear understanding of the fraud risks they face and a statement of how they will deal with those risks. Key operational measures include:

- fraud risk assessment; and
- fraud policy.

Fraud Risk Assessment in a Period of Change

All organisations need to know their key fraud risks. Even in stable organisations, fraud risks can change over time and it is important that regular fraud risk assessments are carried out. A key principle in CIPFA's recently published Code of Practice[6] states:

> *"Fraud risk identification is essential to understand specific exposures to risk, changing patterns in fraud and corruption threats and potential consequences to the organisation and its service users."*

In new and merged organisations, there is pressure to establish and maintain the key operations of the business. This can be complex and time consuming, particularly given the current scale of reorganisation across the NI public sector. Concentration on business continuity can mean that supporting systems, such as governance arrangements and risk assessment, are given a lower priority and may be overlooked in the early months of a new organisation. This can increase opportunities for fraud.

The main elements of a fraud risk assessment process are[7]:

- understanding the business – size, complexity, locations, processes;
- identifying and categorizing fraud risks;
- evaluating fraud risks; and
- addressing fraud risks through a system of controls.

Understanding the business

It is essential that a comprehensive fraud risk assessment is carried out early in the life of a new or merged organisation. Under proposed departmental changes, for example, there will be a significant transfer of functions, and the fraud risks associated with any new functions must be evaluated by the new organisation.

---

6 *Code of Practice on Managing the Risk of Fraud and Corruption*, CIPFA, December 2014

7 *Fraud Risk Management: Developing a Strategy for Prevention, Detection and Response*, KPMG Forensic, 2006

Current changes may also affect the physical spread of an organisation, for example the five education and library boards merging into one education authority. Where there have been offices in five locations carrying out all functions, there may now be one head office with a number of satellite offices, each only carrying out certain functions. Any new organisational structure will have associated fraud risks.

While presenting challenges, a changing business environment also provides an ideal opportunity to address fraud risks at the outset. A report on changes in local government service delivery in England and Wales[8] highlighted that the changing landscape allowed for "fraud proofing" of new systems, policies and delivery models, in effect using the expertise of internal auditors and counter fraud specialists to design fraud out of systems at the earliest opportunity.

Identifying and categorizing fraud risks

In addition to new fraud risks associated with transferred functions and structural change, there are fraud risk factors inherent in the **change process** itself, for example:

- lack of effective Board oversight in the transition period;
- unclear roles and responsibilities in new business areas;
- crisis management in a pressured business environment;
- no established ethical culture or code of conduct for the new organisation;
- staff turnover in key control areas;
- loss of key staff following downsizing; and
- inadequate separation of duties following staff reductions.

Other **general factors** affecting an organisation's vulnerability to fraud risk include:

- the size and complexity of the organisation;
- the nature of the business, for example providing health or education services, administering major capital projects, grant administration or regulation/licensing;
- the adequacy of the control environment;
- the type and value of assets held; and
- the quality and reliability of staffing arrangements, including possible adverse motivational factors.[9]

All of these factors can come to the fore during a major change process. In the case of current changes in the NI public sector, for example, organisations are becoming larger and more complex, control environments are being altered and staffing arrangements are being affected by the need to reduce staff

8 *Fighting Fraud Locally: The Local Government Fraud Strategy*, April 2011

9 *Managing the Risk of Fraud (NI): A Guide for Managers*, Department of Finance and Personnel, December 2011

numbers, with possible consequences in terms of staff morale. The need to identify and categorise fraud risk is therefore heightened. Only when all fraud risks have been identified by the new and merged organisations (see Figure 5) can they be evaluated and prioritised properly.

Figure 5: Identifying Fraud Risks

Fraud risks can be identified in a number of ways, for example:

- conduct fraud risk workshops or self-assessments – staff who implement policies and procedures should have detailed knowledge of potential risks;
- compare/benchmark identified risks with similar organisations;
- commission a fraud risk review e.g. from internal or external auditors or specialist consultants; or
- use external sources and reports which identify key fraud risks for particular sectors or types of business.

Sources: *Code of Practice on Managing the Risk of Fraud and Corruption*, CIPFA, December 2014
Managing the Risk of Fraud (NI): A Guide for Managers, Department of Finance and Personnel, December 2011

Evaluating Fraud Risks

Evaluating fraud risks involves assessing the likelihood of the fraud occurring and the severity of impact if the fraud does occur. This enables fraud risks to be prioritised and aids decision making in terms of putting in place mitigating controls. Although fraud risk increases in periods of significant change, conversely the creation of a new organisation can provide an opportunity to address fraud risk effectively by making new policies, systems and processes resilient to fraud.

Commonly, a **risk matrix** (Figure 6) is used to assess whether the risk is high (red), medium (amber) or low (green). The level of fraud risk will determine the level of intervention needed to mitigate the risk. Values can be assigned to the categories of probability and impact so that each fraud risk has a score or ranking (see examples in Figure 6).

Figure 6: Fraud Risk Matrix

Probability						
	Very High (5)		10			25
	High (4)					
	Medium (3)			9		
	Low (2)	2				10
	Very Low (1)					
		Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
	Impact					

Source: *Policy and Framework for Risk Management*, Department of Finance and Personnel, 2011

The impact of a possible fraud needs to be considered in the widest possible terms. In addition to any financial impact there may be an adverse impact on the organisation's reputation, which could be particularly harmful to a new organisation seeking to become established, or there may be commercial or political sensitivities.

Addressing fraud risks

Having identified and evaluated the full range of fraud risks to which it is exposed, an organisation is then in a position to tackle the risks in a prioritised and proportionate way. The most effective way to address fraud risk is by establishing a system of internal controls to create a strong internal control environment. This is discussed in the next section.

The Audit Committee should be involved in reviewing and challenging the fraud risk assessment and proposed control environment, particularly in new and merged organisations, and reporting on this to the Board. Board oversight at times of significant change is essential for a successful transition.

Fraud Policy

All new and merged public sector organisations should have a **fraud policy** in place which states clearly that **fraud will not be tolerated**, sets out the responsibilities of all staff in relation to fighting fraud and cross-refers to related policies such as the code of conduct, whistleblowing policy and fraud response plan. Department of Finance and Personnel (DFP) guidance (see footnote 9) provides a model policy.

Preventing fraud - Self-assessment checklist

Consider each statement and determine whether it should be assessed as:

Red: The area needs significant strengthening and improvement to reduce fraud risk.
Amber: The area needs some strengthening and improvement to reduce fraud risk.
Green: The area is strong and fraud risk has been reduced to an acceptable level.

Red	Amber	Green	
			Organisational Culture:
☐	☐	☐	Our organisation has a zero tolerance approach to fraud and corruption that is communicated to all staff in a policy. All staff are aware of their role in relation to fraud prevention.
☐	☐	☐	There is clear commitment from senior management and the Board that fraud will not be tolerated.
☐	☐	☐	We have communicated our zero tolerance of fraud to all staff, contractors and other third parties with whom we do business. They know what to do if they become aware of possible fraud.
☐	☐	☐	A designated senior manager has responsibility for counter fraud work, sufficient resources for this work and direct access to the Audit Committee.
☐	☐	☐	There is a code of conduct which sets out clearly for employees which behaviour is acceptable or unacceptable. All staff are required to sign up to this annually. The code highlights that unethical behaviour will lead to disciplinary proceedings.
☐	☐	☐	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.
☐	☐	☐	Our organisation maintains a register of gifts and hospitality. Staff are aware of the need to register any gifts and hospitality received.
☐	☐	☐	All staff attend regular fraud and ethics awareness training. The effectiveness of the training is confirmed through testing. New staff receive fraud and ethics awareness training at induction.
☐	☐	☐	Our organisation undertakes pre-employment screening by risk assessing posts and undertaking checks to minimise the risk of employing dishonest and unethical staff.
☐	☐	☐	Leavers and retirees are subject to an exit interview which is designed to identify any vulnerability to fraud. The Audit Committee is notified of any relevant concerns.
☐	☐	☐	Our organisation has a counter fraud strategy in place, which applies to all aspects of the business, is communicated across the organisation and is overseen by those charged with governance.

Fraud Risk Assessment:

- ☐ ☐ ☐ Our organisation considers fraud risk as part of the overall risk management process.
- ☐ ☐ ☐ Our organisation has carried out a rigorous fraud risk assessment in the last two years (more recently if a new or merged organisation).
- ☐ ☐ ☐ Our assessment of fraud risk is based on known fraud risks, benchmarking with similar organisations and internal brainstorming with frontline staff.
- ☐ ☐ ☐ Our fraud risk assessment has been reviewed and agreed by the Audit Committee and/or Board.
- ☐ ☐ ☐ Counter fraud staff and/or internal audit have a role in fraud-proofing new policies, strategies and initiatives across our organisation to minimise fraud risks.
- ☐ ☐ ☐ Our fraud risk assessment is reviewed at regular intervals, and particularly when our organisation changes, to ensure that any new fraud risks are identified and addressed.

Audit Committee:

- ☐ ☐ ☐ Our Audit Committee takes a proactive role with respect to fraud prevention.
- ☐ ☐ ☐ Our Audit Committee is totally independent of management and includes members with financial expertise.
- ☐ ☐ ☐ Our Audit Committee meets at least quarterly and devotes sufficient time to providing assurance on our counter fraud strategy.

Sources: Adapted from *'Fighting Fraud Locally' voluntary checklist for local authorities*, April 2011, *Fraud Control Frameworks: Best Practice Guide*, UAE State Audit Institution, January 2011 and *Managing the Business Risk of Fraud: A Practical Guide*, ACFE and IIA, June 2008

Detecting fraud

It is impossible to eliminate all fraud through preventative measures without paralysing an organisation, so there will always be a risk of fraud occurring. A **counter fraud strategy** must therefore include measures for detecting fraud. Key detection measures include:

- internal control environment;
- data mining and data matching; and
- whistleblowing arrangements.

Internal Control Environment

The internal control environment of an organisation can both **prevent** and **detect** fraud. Internal controls should be designed to make it more difficult for people to commit fraud in the first place and to pick up instances where fraud has occurred. They should target key risks (as identified in the fraud risk assessment process) and should be proportionate to the level of risk identified. Figure 7 outlines the main types of internal controls.

Figure 7: Types of Internal Controls

Directive controls

Directive controls are about directing behaviour in order to minimise the risk of fraud. Examples include procedure manuals or checklists for the various processes within an organisation, or imposing spending limits for particular programmes or projects.

Preventive controls

Preventive controls are designed to reduce the likelihood of fraud happening. Examples of preventive controls include: separation of duties, which ensures that one person does not carry out all elements of a process; authorisation of transactions by supervisors; fraud awareness training for all staff; and physical security of key assets.

Detective controls

Detective controls are designed to detect fraud and errors after they have occurred. Examples include bank reconciliations, comparing actual spend with budgets, exception reports and periodic audits.

Corrective controls

Corrective controls involve restoring a system or process after a fraud has occurred, for example using back-up tapes to restore an IT system after it has been breached.

Source: *Managing the Risk of Fraud (NI): A Guide for Managers*, Department of Finance and Personnel, December 2011

Priority should be given to preventive and directive controls which are designed to stop fraud happening. **Appendix 1** outlines risks and controls for specific key areas.

It is essential not only that effective controls are in place but that they are operating as they should. DFP's latest Annual Theft and Fraud report[10] highlights that in 13 per cent of reported fraud cases, the fraud was caused either by inadequate controls (4 per cent) or failure to apply existing controls (9 per cent).

Fraudsters are continually looking for ways to circumvent established controls so the effectiveness of controls needs to be reviewed regularly.[11] In a time of significant change, fraudsters may see an increased opportunity for breaching long established controls which they perceive to be weakened.

The following two **case examples** highlight how organisations are susceptible to both internal and external fraud where inadequate controls are in place or where existing controls are not properly applied.

10 *Annual Theft and Fraud Report 2013-14*, DFP

11 *Tackling External Fraud*, HM Treasury and National Audit Office, 2008

Case Example - Ordnance Survey of Northern Ireland (OSNI)

In August 2003, OSNI uncovered an internal fraud in its Accounts Branch which had been perpetrated over a five year period and defrauded OSNI of £70,690. The fraudster 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. He was formally charged by the Police with stealing cash and falsifying records. He pleaded guilty and was sentenced to twelve months imprisonment, suspended for two years. The fraud occurred because of inadequate separation of duties and was discovered when the perpetrator went off on extended sick leave and was unable to cover his tracks.

Source: *Internal Fraud in Ordnance Survey NI*, Northern Ireland Audit Office, 15 March 2007

Case Example - Belfast City Council

In July 2013, Belfast City Council was the victim of an external fraud involving changes being made to bank account details for one of its main contractors. This resulted in two payments, totalling more than £292,000, being made to a fraudulent bank account. The Police investigation concluded that there was no evidence that either Council staff or employees of the Contractor were involved in the fraud. However, an internal review by the Council's Audit Governance and Risk Services found that had existing controls been followed, the fraud would not have occurred. Follow up actions included a review of procedures and the introduction of additional management checks. The Council recovered most of the loss from its insurers.

Source: *Local Government Audit Report 2014*, Northern Ireland Audit Office, November 2014

Internal control environment in a new or merged organisation

The fraud risks associated with a process of change (see page 15) should be given particular attention by new and merged organisations when establishing their internal control environment (see Figure 8).

Figure 8: Fraud Risk and the Change Process

Fraud Risk	Mitigating Controls
Lack of effective Board oversight in the transition period	• A clear change management strategy which emphasises the key role of Board members • Early appointment of new Board members so there is no gap in governance • Additional Board meetings during the transition period
Unclear roles and responsibilities in new business areas	• Clearly documented roles and responsibilities • Documented procedures and processes • Clear communication
Crisis management in a pressured business environment	• Clearly documented change management strategy setting out key priorities • Clearly documented roles and responsibilities • Senior management involvement in change management
No established ethical culture or code of conduct for the new organisation	• An early statement from the Board and senior management of the new organisation that fraud will not be tolerated • Early issue of the new organisation's code of conduct which staff should be asked to sign up to as soon as possible • Staff awareness training
Staff turnover in key control areas	• Documented procedures • Staff training and awareness • Increased supervisory checks
Loss of key staff following downsizing	• Documented procedures • Staff training and awareness • Increased supervisory checks
Inadequate separation of duties following staff reductions	• Clearly documented roles and responsibilities • Increased supervisory checks

Internal control and internal audit

Internal audit does not have a direct role in detecting fraud but does have expertise in risk management and controls. Internal audit can provide independent, objective advice to management on fraud risks and the controls which should be in place to mitigate those risks. Internal audit can also play a valuable role in reviewing new policies and programmes so that fraud risk can, as far as possible, be minimised at the outset. This may be particularly relevant for new and merged organisations.

Data Mining and Data Matching

Organisations hold a wealth of data (much of it electronically) which can be used to help prevent and detect fraud. Computer software and technology can analyse or compare large amounts of data both within and across organisations. The need for collaborating and sharing information across organisations to help in the fight against fraud has been highlighted by the UK Government.[12]

Data mining involves using computerised techniques to analyse electronic data.[13] It can be used on a continuous basis or for ad hoc exercises. For example, analysing trends in transactions can highlight unusual patterns, gaps or duplicates which could be indicators of fraudulent activity. Techniques used for data mining and data analysis need not be costly or complex and might include spreadsheet queries or audit software such as IDEA.[14]

In times of significant change, for example with the creation of new organisations or the merger of existing organisations, the value of data mining and analysis may be temporarily restricted because historic patterns of expenditure or transactions have been terminated and new patterns will take time to become established in the new or merged organisation. This is also the time when potential fraudsters may exploit uncertainty to perpetrate fraud. The controls outlined at Figure 8 are therefore essential to combat any heightened risk.

Data matching involves comparing sets of data within or across organisations in order to highlight inconsistencies which may indicate fraud. Examples of data that may be matched are payroll, pensions, creditor payments and benefits records. The National Fraud Initiative (NFI) is one of the UK's biggest data matching initiatives[15] used to prevent and detect fraud and the majority of public sector organisations in Northern Ireland submit their data for matching as part of the NFI.

12 *Eliminating Public Sector Fraud: Counter Fraud Taskforce Interim Report*, Cabinet Office, June 2011 and Tackling Fraud and Error in Government, HM Government, February 2012

13 *Fraud Facts: An Introduction to Fraud Detection*, Fraud Advisory Panel, April 2011

14 IDEA is a data analysis tool used by auditors, accountants and finance professionals.

15 The NFI is governed by a Code of Data Matching Practice to ensure compliance with the Data Protection Act.

The following **case examples** illustrate the value of data matching.

Case Example – National Fraud Initiative

Matching of benefits and payroll data showed that a person was claiming benefits while working for two public sector organisations. Overpayment of benefits amounted to around £47,000 over a period of six years. The person was sentenced to nine months' imprisonment, suspended for two years. A recovery plan is in place.

Case Example – National Fraud Initiative

An address match between benefits and payroll revealed that a benefit claimant had failed to declare that they were living with a public sector employee. Overpayment of benefits in an eight year period amounted to almost £68,000. The claimant was sentenced to 18 months' imprisonment, suspended for three years, and is repaying the amount by monthly instalments.

Source: *The National Fraud Initiative: Northern Ireland*, Northern Ireland Audit Office, June 2014

Case Example – Local Enterprise Development Unit (LEDU)

An accounts clerk in LEDU diverted £118,000 of public money into her personal bank account by creating two fictitious supplier accounts using her own bank account details. The fraud was discovered by LEDU's Assistant Accountant following a data matching exercise which compared the bank details of suppliers and LEDU staff. The fraudster was able to perpetrate the fraud by bypassing controls, manipulating other staff and opening accounts without proper authority. She was sentenced to two years in prison.

Source: *NIAO Appropriation Account Volume 2000-01*, Northern Ireland Audit Office

As new and merged organisations become established, it is important that they explore ways in which data mining and data matching can help in their fight against fraud.

Whistleblowing Arrangements

Employees are often the "eyes and ears" within an organisation and therefore an invaluable resource in helping to detect fraud. As part of an open and ethical culture, staff should be **encouraged to raise concerns** about possible fraud and it is essential that they have a secure and reliable means of doing so. Whistleblowing arrangements[16] should be in place which set out clearly and simply how, and to whom, staff should report suspicions of fraud.

As new organisations are formed or existing organisations merge, and consequently fraud risk increases, it is important that whistleblowing arrangements are reviewed and revised to reflect, for example, changes in contact details, and to ensure that reporting channels remain valid. Staff should be made aware of any new arrangements or points of contact. Figure 9 sets out the key elements of a successful whistleblowing policy.

Figure 9: Key elements of a whistleblowing policy

A whistleblowing policy should include:

- commitment from the top of the organisation that concerns will be welcomed and treated seriously;
- a range of options for reporting concerns, both inside and outside the organisation;
- a clear process for raising concerns, perhaps represented diagrammatically for ease of reference;
- assurances about confidentiality, which should be protected as far as possible;
- details on how to access independent advice and support, such as Public Concern at Work;
- clear procedures on how management will handle concerns raised; and
- reassurance that employees will not be victimised or suffer detriment for raising concerns.

Source: *Review into Government Whistleblowing Policies*, National Audit Office, January 2014

Service users and members of the public should also be encouraged to raise concerns. New and merged organisations should provide details on their website of how this might be done, for example via a dedicated email address or hotline telephone number.

Recording and analysing whistleblowing concerns can provide organisations with useful information about possible system weaknesses. Whistleblowing concerns should be collated and reported to the Audit Committee.

16 Detailed guidance on whistleblowing arrangements can be found in *Report on the Effectiveness of Existing Arrangements for Workplace Whistleblowing in the UK*, Public Concern at Work Whistleblowing Commission, November 2013 and in *Whistleblowing in the Public Sector: A Good Practice Guide for Workers and Employers*, UK Audit Agencies and Public Concern at Work, November 2014

The following case example highlights the potential consequences of not properly addressing whistleblowing concerns.

Case Example – Bytel

A project for a high speed cross-border broadband link was delivered by Bytel Ltd, a Belfast-based IT company. It was part grant funded under an EU programme delivered by the Special EU Programme Body (SEUPB), with the Department of Enterprise, Trade and Investment (DETI) appointed as one of two Joint Implementing Agents.

The Public Accounts Committee (PAC) reported in June 2015 on the handling of this project. It found that DETI received allegations about the project from a whistleblower in 2006, including:

- Bytel had used a sister company to order equipment for the project; and
- Bytel had claimed grant for assets which it did not own.

Although DETI investigated the allegations at the time, PAC found that the investigation was fundamentally flawed because it was carried out by the same staff who had overseen the delivery of the project and checked Bytel's grant claims. The Committee said this lack of independence made the investigation ineffectual. Following further whistleblowing allegations in 2008, DETI considered carrying out an investigation to PACE (Police and Criminal Evidence) standards but this was never commissioned.

SEUPB was not made aware of the whistleblowing allegations until 2011 and then commissioned a full forensic review of the project, which was completed in 2012. The forensic review was not completed to PACE standards. PAC said that consequently *"there is a lack of clarity about who bears responsibility for the shortcomings and whether there was any misconduct or criminal activity by individuals inside or outside DETI."*

Grant paid should have been 35 per cent of eligible costs (€0.3 million) but assistance of €4.3 million was actually paid, which PAC described as "a totally unacceptable outcome".

PAC recommended that DETI commission a PACE investigation of the Bytel project as a matter of urgency.

Source: *Report on the cross-border broadband initiative: the Bytel project*, Public Accounts Committee, NIA 253/11-16, June 2015

Detecting fraud - Self-assessment checklist

Consider each statement and determine whether it should be assessed as:

Red: The area needs significant strengthening and improvement to reduce fraud risk.
Amber: The area needs some strengthening and improvement to reduce fraud risk.
Green: The area is strong and fraud risk has been reduced to an acceptable level.

Red	Amber	Green	
			Internal Control Environment:
☐	☐	☐	Our internal controls have been designed to address identified fraud risks and help prevent fraud occurring. The controls are proportionate to the identified fraud risks.
☐	☐	☐	Our internal control environment includes a range of complementary controls (directive, preventive, detective and corrective).
☐	☐	☐	All staff, contractors and other stakeholders are made aware that there are controls in place to prevent and detect fraud, as a deterrent.
☐	☐	☐	Our fraud risk controls have been reviewed by internal audit and the Audit Committee.
☐	☐	☐	Internal audit has a direct role in reviewing any new or amended policies and programmes to ensure that fraud risk is minimised at the outset.
☐	☐	☐	Internal audit tests controls to mitigate fraud risks as part of its annual programme of work.
			Data Mining and Data Matching:
☐	☐	☐	We regularly use data analysis to detect potentially fraudulent activity.
☐	☐	☐	Our IT and information systems include controls (such as reconciliations, physical counts and analyses) designed to detect potentially fraudulent activity.
☐	☐	☐	Our data analysis controls include review of journal entries, unusual transactions and period-end transactions, where fraud may be concealed by management override.
☐	☐	☐	We share data and participate in data matching exercises (e.g. the National Fraud Initiative) to help in the prevention and detection of fraud.
☐	☐	☐	We act promptly on any issues of concern identified through data mining and data matching.

Whistleblowing arrangements:

☐	☐	☐	Our organisation has an internal whistleblowing policy and procedures in place which are known to all staff. Staff are regularly reminded of the policy and procedures.
☐	☐	☐	Our whistleblowing arrangements are endorsed by senior management and the Board, and include an assurance that all concerns raised will be welcomed and treated seriously.
☐	☐	☐	The policy and procedures make clear how, and with whom, staff should raise concerns about possible fraud. A range of internal and external reporting options is given.
☐	☐	☐	The policy and procedures make clear how we will handle any concerns raised.
☐	☐	☐	Our whistleblowing policy provides reassurance that employees will not be victimised or suffer detriment for raising concerns. We monitor to ensure this commitment is borne out in practice.
☐	☐	☐	Our whistleblowing policy provides assurance about confidentiality. Confidentiality is respected as far as possible in practice.
☐	☐	☐	Our whistleblowing policy allows for anonymous disclosures, which will be treated seriously, but points out the disadvantages of anonymous disclosures.
☐	☐	☐	There is a clear process by which contractors, third parties and members of the public can raise concerns about possible fraud in our organisation, for example a fraud hotline. Details are easily accessible on our website.
☐	☐	☐	We review our whistleblowing arrangements periodically to ensure their continued effectiveness. We seek views from employees as to their level of trust and confidence in the arrangements.
☐	☐	☐	We maintain confidential case files on all concerns raised and analyse the caseload for indications of systemic control weaknesses.
☐	☐	☐	We report on whistleblowing caseload to the Audit Committee.

Sources: Adapted from *'Fighting Fraud Locally' voluntary checklist for local authorities*, April 2011, *Fraud Control Frameworks: Best Practice Guide*, UAE State Audit Institution, January 2011 and *Managing the Business Risk of Fraud: A Practical Guide*, ACFE and IIA, June 2008

Responding to fraud

A key part of a counter fraud strategy is having in place an **effective response to fraud** when it occurs. Dealing with fraud effectively provides a deterrent effect and shows that an organisation is serious about learning from frauds that occur so that fraud risk can be minimised in the future. This should be a key objective for all new and merged organisations.

A **fraud response plan**[17] is an essential document for all organisations. For newly formed or merged organisations, it is important to set the tone as early as possible by establishing and communicating a fraud policy and fraud response plan (see Figure 10) to all staff.

Figure 10: Fraud Response Plans

Fraud response plans should:

- outline the entire fraud investigation process from receipt of the initial allegation through to the final outcome report;
- clearly define the roles and responsibilities of senior management and others involved in the investigation process;
- outline procedures for securing evidence and undertaking interviews;
- set out arrangements for dealing with staff under suspicion;
- include arrangements for when, and how, to contact the police;
- commit to pursuing the full range of sanctions – disciplinary, regulatory, civil and criminal;
- make clear that recovery action will be taken in relation to all fraud losses;
- set out fraud reporting arrangements both within the organisation (for example, to senior management and the Audit Committee) and externally to relevant third parties (for example, regulators or auditors); and
- clarify how lessons learned from frauds will be used to strengthen controls to prevent recurrence.

Source: *Managing the Risk of Fraud (NI): A Guide for Managers,* Department of Finance and Personnel, December 2011
Fraud Facts: An introduction to fraud response plans, Fraud Advisory Panel, July 2010

Fraud Investigations

Fraud investigation is a specialised area and must be undertaken by appropriately trained and qualified staff if it is to be effective. The fraud response plan should emphasise the need for **fraud investigation expertise** and outline how any skills gap will be filled, for example by buying in appropriate resources.

17 For detailed guidance, see *Managing the Risk of Fraud (NI): A Guide for Managers*, Department of Finance and Personnel, December 2011, Appendix 2

If a criminal act is suspected, the fraud response plan should specify arrangements for liaising with the police. Key considerations for fraud investigations are outlined at Figure 11.

Figure 11: Fraud Investigations

Organisations must ensure that:

- investigations are carried out in accordance with clear guidance, normally the fraud response plan;
- those undertaking the investigation are trained in fraud investigation techniques, have the necessary powers and are totally independent of the area under investigation;
- investigations are timely;
- full consideration is given in the investigation process to:
  - » maintaining confidentiality;
  - » protecting evidence;
  - » interviewing witnesses and suspects;
  - » liaising with the police, other experts and regulators as appropriate;
  - » the need for expert advice from, for example, forensic accountants or asset recovery specialists;
  - » reporting progress and findings to senior management;
  - » preparing media statements if required; and
  - » managing any civil proceedings to recover assets lost.

Source: *Managing the Risk of Fraud (NI): A Guide for Managers,* Department of Finance and Personnel, December 2011
Fraud Facts: An introduction to fraud response plans, Fraud Advisory Panel, July 2010

The following case example highlights what can go wrong in fraud investigations, and the need for appropriate investigation expertise.

Case Example – Department for Regional Development

The NI Assembly's Public Accounts Committee (PAC) reported on two cases where fraud investigations were overseen by the Department for Regional Development (DRD):

- Internal auditors identified a case of "invoice slicing" in NI Water, whereby a manager instructed a contractor to limit the value of invoices submitted for payment to below £20,000, thereby avoiding more rigorous approval levels.
- A whistleblower made allegations against DRD's Roads Service in relation to collusion and favouritism in awarding contracts for road signs.

In both cases, investigations found no evidence of fraud.

PAC identified a number of fundamental weaknesses in how these two cases were investigated:

- The investigations were conducted by internal auditors with little experience in investigating fraud and no relevant fraud training.
- The investigations had flawed terms of reference and inadequate planning, and inappropriate investigative methodologies were used.
- Record keeping was poor.
- The investigations were not driven by the need to prove a specific breach in the law and gather evidence capable of supporting a criminal prosecution.
- There was a lack of professional scepticism and a readiness to accept irregularities as human error or systems weaknesses rather than indicators of fraud.
- There was a lack of engagement with the police or other fraud specialists.
- There was a failure to take whistleblower concerns seriously and properly investigate allegations.

PAC recommended that only suitably qualified and experienced staff should lead fraud investigations. It also recommended that investigative capacity in the public sector should be strengthened through the establishment of a centralised fraud investigation service.

Source: *Report on NI Water's Response to a Suspected Fraud and DRD: Review of an Investigation of a Whistleblower Complaint*, Public Accounts Committee, NIA 172/11-15, April 2014

Within the NI public sector there are a number of specialist fraud investigation units, for example in relation to benefit fraud, legal aid fraud and health service fraud. Following recommendations by the Public Accounts Committee about the need to improve the quality of fraud investigations in other parts of the NI public sector, DFP has established a Group Fraud Investigation Service which can be used by NI departments, agencies and arm's length bodies.

Sanctions and Redress

Responding to fraud by **applying sanctions** and seeking **recovery of any losses** helps send out a strong message that fraudsters will not benefit by their actions, and provides a powerful **deterrent effect** to other potential fraudsters. A sanction is a penalty or enforcement action taken against someone who has committed fraud. A range of sanctions may be applied (see Figure 12).

Figure 12: Types of Sanctions

- **Disciplinary** – an internal procedure against a member of staff who has committed fraud. For example, this could be a written warning, suspension, demotion or dismissal.
- **Regulatory** – a sanction against an individual or an organisation. Where a fraudster holds an accreditation or licence to practice, for example health professionals, there may be a sanction through their regulatory body.
- **Civil** – an action in civil law seeking damages or compensation from the fraudster.
- **Criminal** – prosecution of fraudsters, in most cases involving the police.

Sources: *Fraud Facts: An overview of parallel sanctions*, Fraud Advisory Panel, August 2010
Fraud and Punishment: enhancing deterrence through more effective sanctions, Centre for Counter Fraud Studies, University of Portsmouth, July 2012

It is important that new and merged organisations include a clear statement in their fraud response plans that they will apply all possible sanctions and seek to recover all losses. This statement must be backed up by **decisive action** when a fraud occurs. Where appropriate, organisations should consider applying **parallel sanctions**, for example internal disciplinary proceedings alongside a civil action.

The following **case example** illustrates how an unsatisfactory response to possible fraud can jeopardise the chances of securing a prosecution and redress for losses suffered.

Case Example - Belfast Education and Library Board (BELB)

In August 2005, a new Facilities Manager at the BELB raised concerns about the amount of work being offered to a particular contractor. The work was required to bring libraries into compliance with the access requirements of disability legislation. A site visit revealed that the BELB had paid £80,000 for work at two libraries which had not been completed. When the BELB reviewed similar work undertaken in 14 other libraries, it found that £110,000 had been paid for work which either was not carried out or was not carried out to the required standard.

A subsequent investigation identified that the maintenance officer had allocated the contracts without seeking quotations or going to tender and had authorised payments to the contractor. He then alleged that documents relating to the library work had been stolen from his car. The maintenance officer was initially suspended then had his employment terminated in August 2007 on ill-health grounds.

There were strong suspicions of fraud in this case, even though extensive investigations were unable to establish evidence which would support criminal prosecutions.

The Public Accounts Committee (PAC) found that while the BELB had received a wide range of anti-fraud and procurement guidance, this had not been followed in the case in question, and an anti-fraud policy and fraud response plan had not been fully implemented. PAC found that the failure to implement proper procedures and the absence of documentation had undermined the prospect of criminal charges, which made redress more difficult. However, the Committee stressed the importance of taking every possible action to recover sums overpaid or sums paid for work not done.

Sources: *The Investigation of Suspected Contract Fraud*, Northern Ireland Audit Office, 29 April 2009
Report on the Investigation of Suspected Contract Fraud, Public Accounts Committee, First Report of Session 2009-10, July 2009

Fraud reporting and case review

Increased fraud risk during periods of significant change may lead to increased levels of actual and attempted fraud. Frauds which occur provide opportunities to learn from system weaknesses or poor controls. New and merged organisations must identify the control failures that allowed the fraud to happen in the first instance and put in place modified or additional controls to prevent recurrence. **Reporting fraud internally** to the Board and Audit Committee ensures that any lessons to be learned are endorsed at the highest level and shared across the organisation. In addition, new and merged

organisations should establish arrangements for reporting annually to the Board and Audit Committee, as outlined in Figure 13.

Figure 13: Annual Fraud Reporting

Information provided to the Board and Audit Committee could include:

- a summary of all fraud cases in the year (number, type of fraud and value);
- how the frauds occurred (e.g. absence of controls, failure to apply controls);
- how the frauds were discovered (e.g. whistleblowing, normal operation of controls, internal audit);
- the outcomes of internal investigations;
- the status of cases passed to external agencies for investigation;
- a summary of sanctions imposed and losses recovered; and
- changes made to internal control systems to prevent recurrence.

Sources: *Managing Public Money Northern Ireland*, DFP, June 2008 and *FD (DFP) 03/15*
Fraud Control Frameworks: Best Practice Guide, UAE State Audit Institution, January 2011

Organisations may also be required to report fraud externally to, for example:

- sponsor departments;
- the police;
- insurers;
- regulatory authorities;
- banks; and
- external auditors.

A key element of reporting fraud externally is to allow the wider impact of the fraud to be determined and lessons learned to be shared appropriately across sectors.

NI departments and their arm's length bodies must report all frauds[18] (including attempted frauds) to DFP and the Comptroller and Auditor General (C&AG). DFP uses the information to prepare an annual report on fraud trends across the central government sector and to issue fraud alerts and additional guidance as appropriate. The C&AG uses the information to determine the impact of fraud on the financial accounts of the central government organisations which he audits.

18 *Managing Public Money Northern Ireland*, DFP, June 2008, paragraph A.4.7.8

Responding to fraud - Self-assessment checklist

Consider each statement and determine whether it should be assessed as:

Red: The area needs significant strengthening and improvement to reduce fraud risk.
Amber: The area needs some strengthening and improvement to reduce fraud risk.
Green: The area is strong and fraud risk has been reduced to an acceptable level.

Red	Amber	Green	
			Fraud Response Plan
☐	☐	☐	Our organisation has a comprehensive fraud response plan in place. The plan is approved by the Audit Committee and Board.
☐	☐	☐	The fraud response plan makes clear that all allegations of fraud will be investigated and appropriate action taken.
☐	☐	☐	All allegations of fraud, including anonymous allegations, are assessed in line with the fraud response plan.
			Fraud Investigations
☐	☐	☐	The fraud response plan clearly documents the procedures for fraud investigations.
☐	☐	☐	All fraud investigations are carried out in accordance with the fraud response plan.
☐	☐	☐	There are arrangements in place for securing fraud investigation expertise from outside the organisation, if required.
			Sanctions and Redress
☐	☐	☐	In responding to proven fraud, we consider the full range of possible sanctions – disciplinary, regulatory, civil and criminal. Where appropriate we consider parallel sanctions.
☐	☐	☐	The fraud response plan makes clear that we will seek to recover any losses incurred due to fraud.

Fraud Reporting and Case Review

☐	☐	☐	All frauds are brought to the attention of the Board and Audit Committee.
☐	☐	☐	We review and strengthen systems and controls in light of proven frauds.
☐	☐	☐	We report annually to the Board and Audit Committee on fraud caseload.
☐	☐	☐	We report all frauds to external third parties as required.
☐	☐	☐	We publicise proven frauds, and action taken in response to the frauds, both internally and externally as appropriate, as a deterrent.

Source: Adapted from *'Fighting Fraud Locally' voluntary checklist for local authorities*, April 2011, *Fraud Control Frameworks: Best Practice Guide*, UAE State Audit Institution, January 2011 and *Managing the Business Risk of Fraud: A Practical Guide*, ACFE and IIA, June 2008

Appendix 1

Fraud Risks and Controls

This Appendix outlines examples of areas which may be susceptible to increased fraud risk in times of change and the mitigating controls which organisations should ensure are in place and operating effectively.[19]

Payroll and Employee Fraud

Current changes across the NI public sector may expose organisations to an increased risk of payroll fraud, as a result of merging workforces and staff reductions through voluntary exit schemes. Downsizing and potential loss of key staff may also impact on separation of duties and supervisory checks. The scale of change could impact on staff morale, leading to an increased risk of employee fraud. The table below sets out potential risks and mitigating controls.

Risks	Key controls
Payroll fraud • The creation of fictitious or 'ghost' employees • Inadequate separation of duties • Unauthorized amendments to input data e.g. pay rate alteration • Prolonging the pay of a leaver and/or diverting their pay into a fraudster's account • Excessive overtime payments or bonuses	• Access to payroll systems by authorised personnel only • Segregation of duties between those who authorise appointments, change standing data and action payments • Clear procedures in place for processing starters, leavers and other payroll changes, including review and authorisation of all changes on each payroll run • Checking of exception reports by management • Data matching checks for duplicate names, addresses and bank account details • Periodic HR check of payroll master file • Reconciling payroll spend with budget to highlight any unexplained variations
Employee fraud • Submission of false or inflated expenses claims (including excess fares allowance on relocation) • Bogus time recording • The abuse of sickness absence	• Comprehensive rules on travel expenses and allowances which are clearly communicated and easily accessible to staff and authorising managers • Checks by authorising officers of expenses claims against approved work plans and standard mileages for regular destinations • Original supporting documentation for all claims, such as rail tickets, hotel bills and parking receipts • Periodic checks to protect against misuse of sickness absence e.g. employees working elsewhere when on extended sick leave

19 The key source for this Appendix is *Managing the Risk of Fraud (NI): A Guide for Managers*, Department of Finance and Personnel, December 2011. The Guide provides further detail.

Payments and cash handling

Payments systems and cash handling are key fraud risk areas within organisations. The significant changes within the NI public sector may heighten the risk, as organisations merge and bring together their supplier systems.

Risks	Key controls
• Unauthorised amendments to payee standing data, e.g. bank details, payroll details • Unauthorised use of cheques and payable orders • False or duplicate invoices designed to generate improper payments • Income received but not brought to account • Falsified accounting records • Theft of cash	• Clearly documented roles and responsibilities • Proper authorisation of any changes to standing data • Restricted access to systems for processing changes and secure password controls • Ensure all financial stationery is properly secured and controlled • Separation of duties between those setting up accounts, those ordering and receiving goods and services and those authorising payments • Separation of duties between those receiving income, preparing lodgments, banking cash and cheques and performing bank reconciliations • Use of sequential receipts • Rotation of staff with cash handling duties • Regular random checks on cash balances, source documentation and bank reconciliations • Keep cash balances to a minimum and hold cash securely at all times • Restrict access to cash

Management of physical assets

Significant organisational change can quickly lead to asset records becoming inaccurate. For example, assets may be reassigned to a new or merged organisation, making asset registers and asset tags invalid. Or it may no longer be clear who has responsibility for which assets. Uncertainty surrounding arrangements for asset management weakens control and may provide increased opportunity for theft of attractive items.

Risks	Key controls
• Inaccurate, incomplete or out of date asset registers and logs • Incomplete or inaccurate tagging of assets • Unclear responsibility for assets • Unapproved removal or disposal of assets • Theft of assets • Assets used for personal gain	• All new or merged organisations should ensure that their assets are accurately recorded in new or revised asset registers. This may include the recoding of any land and buildings held as assets • All assets should be marked or tagged as belonging to the new or merged organisation • Responsibility for assets should be assigned as appropriate and responsibilities made clear to assignees • Regular inventory checks and reconciliations should be carried out, particularly of small attractive items • Where appropriate, assets should be stored securely • There should be clear procedures for asset management, from acquisition through to disposal

Contracts and Procurement

All public sector organisations will have contracts in place to secure the goods and services they need to operate. The scale of change across the NI public sector, with some organisations ceasing to exist, new organisations being created and others splitting and merging, will impact on current and future procurement arrangements. Contracts may need to be renegotiated or realigned to new organisational structures and responsibilities. Downsizing of the public sector workforce may lead to the loss of procurement expertise. There will therefore be increased fraud risk at each stage of the procurement cycle – from identifying and specifying the need for the goods/services, through to tendering and award of contract, contract management, ordering and receipt of goods and payment of contractors and suppliers. Examples of risks and controls are set out below.

Risks	Key controls
Contracts	
• Favouritism due to inconsistent application of tender procedures • Inadequate evaluation of contractors and tenders • Manipulation of select lists of contractors • Misuse of single tender actions • Lack of trained procurement and contract management staff • Undeclared conflicts of interest • Collusion between procurement staff and contractors • Inadequate separation of duties • Payment for work not completed • Duplication of contracts (following merger) • Unauthorised contract variations	• Clear procurement policy and procedures based on good practice • Comprehensive evaluation criteria for contractors and tenders, consistently applied • Project Board approval of successful contractor • Access to expertise on procurement and contract management • Procedures for declaring, recording and dealing with potential conflicts of interest • Effective separation of duties or increased supervisory checks where this is not possible • Independent evaluation and authorisation of work completed, prior to payment • Central register of approved and authorised contracts in progress, subject to periodic review • Proper authorisation of contract variations

Risks	Key controls
Procurement	
• Non-sequential purchase orders (increased risk where purchase order systems are being merged) • Inadequate separation of duties • Goods ordered (or misappropriated from stock) for personal gain • Payment for goods not received • Misuse of official procurement cards or credit cards	• Establish a single sequentially numbered purchase order system • Effective separation of duties between ordering goods, receiving goods, approving and paying invoices. Increased supervisory checks where this is not possible • Ensure all invoices are matched to orders before authorisation for payment • Check delivery notes to orders. Only pay for goods delivered • Establish a single authorised signatory list with authorisation limits • Regular stock checks and up-to-date stock records • Ensure only authorised staff can amend standing data, such as supplier records • Regular reports to budget holders to reconcile expenditure to budget • Limit access to procurement and credit cards to specific authorised staff

Grant Funding

A wide range of grants, benefits, allowances and subsidy payments are made to individuals and organisations through a variety of government agencies. The payment of grants is susceptible to external fraud by grant claimants and internal fraud by staff. With loss of staff and changing responsibilities across the NI public sector, it is important that appropriate risk based controls in relation to grant administration are maintained.

Risks	Key controls
• False applications, e.g. inventing an organisation or providing false information on a grant claim • False claims, e.g. where false supporting documentation is provided • Grant not used for the purpose given • Double funding, e.g. non-disclosure of other funding sources • Misappropriation of payments, e.g. through alteration of cheques or changes of bank account details • Non-compliance with conditions of grant, e.g. selling off funded assets • Internal fraud by grants staff, e.g. false applications for personal gain or collusion with a grant applicant	• Establish clear processes and procedures for grant administration and ensure grant staff are fully trained • Perform checks to establish that grant claimant is bona fide, e.g. web searches, checks with relevant regulators, review of key documentation • Pay grant by instalments to reduce risks • Include wording on application forms about the consequences of fraud, as a deterrent • Request full supporting documentation for all grant claims, e.g. invoices, receipts, bank statements • Ensure accuracy and completeness all supporting documentation and validity of all items claimed • Carry out site visits where appropriate • Liaise with other grant paying organisations to reduce risk of double funding • Ensure separation of duties between approving grants, checking grant claims and authorisation of payments

Information and IT

Significant changes across the NI public sector will have potential consequences for information and information technology across organisations. Standing information in relation to staff, suppliers and contractors may change, leading to increased fraud risk around change controls. As organisations merge, there may be implications for IT hardware and software, and relevant controls will need to be reviewed and revised.

Risks	Key controls
• Unclear roles and responsibilities for information and IT in new and merged organisations • Outdated policies and procedures in relation to information and IT • Unauthorised amendments to standing information • Unauthorised disposal of IT equipment	• Clear roles and responsibilities for key staff (information risk owners, IT security officers etc) • Revised and updated policies on information and IT • Access controls to key information and IT systems • Removal of access rights for staff who have left • Change control/usage logs to facilitate management review • Contingency arrangements for recovering and restoring lost data • Proper authorisation of all equipment disposals • Updated inventories and asset tagging of IT equipment

Cyber Fraud

A rapidly growing risk for all organisations, including those in the public sector, is cyber fraud. A wealth of key business information is held on-line and processed on-line, leaving it open to fraud risk from both inside and outside the organisation. The risk of cyber fraud cuts across each of the key business areas covered in this Appendix. In a period of significant change, there may be increased opportunites for those seeking to gain fraudulently from a cyber attack on a new or merged organisation's information, systems and processes.

Risks	Key controls
• Unclear roles and responsibilities for cyber risk management in new and merged organisations • Weakened network security during organisational change and transition • Unnecessary functionality retained on new/ merged systems • Outdated or incorrect user privileges	• A strong governance framework for risk management, including cyber risk, with Board involvement • Security controls testing and penetration testing of network during vulnerable period • Establish an incident response and disaster recovery capability • Unnecessary functionality on ICT systems should be removed or disabled • User privileges should be reviewed and updated as necessary, and user activity monitored

Detailed guidance on cyber security and cyber risk has been produced by the Cabinet Office and the Department for Business, Innovation and Skills and is available on their websites.

Appendix 2

Useful references

An introduction to fraud detection, Fraud Advisory Panel, April 2011

An introduction to fraud response plans, Fraud Advisory Panel, July 2010

An introduction to fraud risk management, Fraud Advisory Panel, July 2010

An overview of parallel sanctions, Fraud Advisory Panel, August 2010

Audit and Risk Assurance Committee Handbook (NI), DFP, March 2014

Fighting Fraud Locally: The Local Government Fraud Strategy, April 2011

Fraud and Punishment: enhancing deterrence through more effective sanctions, Centre for Counter Fraud Studies, University of Portsmouth, July 2012

Fraud Risk Management: Developing a Strategy for Prevention, Detection and Response, KPMG, 2006

Fraud Risk Management: A Guide to Good Practice, Chartered Institute of Management Accountants, 2008

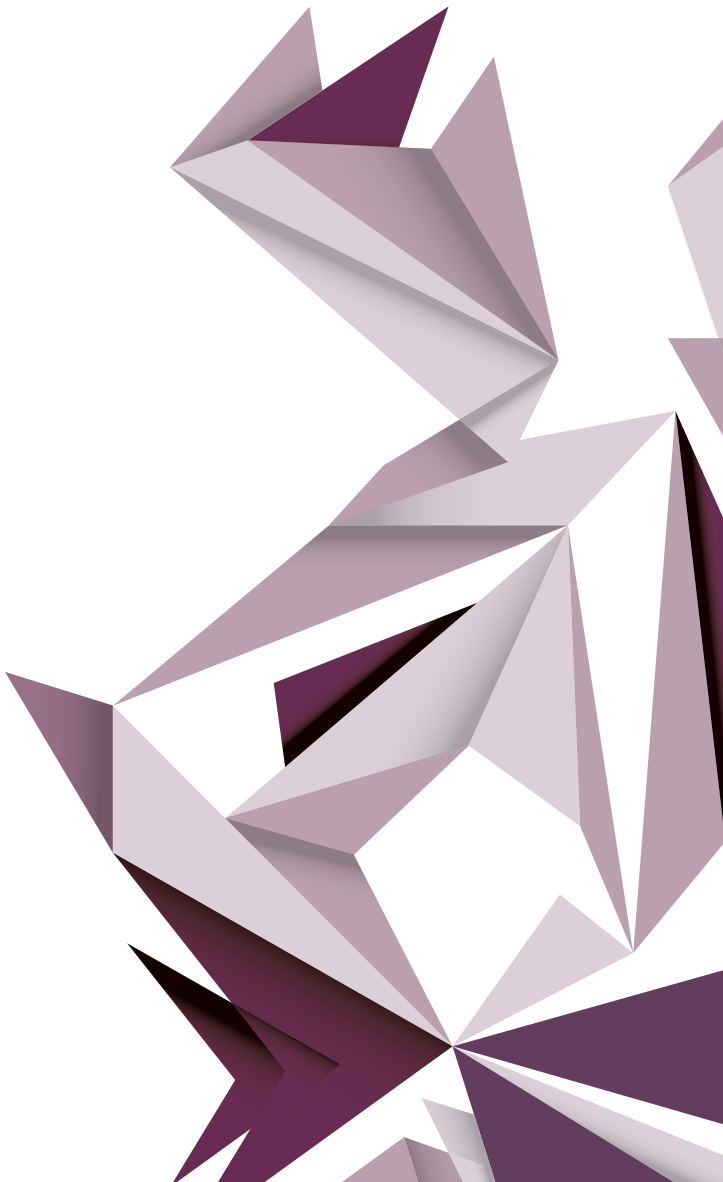
Managing the Risk of Fraud (NI): A guide for Managers, DFP, December 2011

Managing the Risk of Fraud and Corruption, Code of Practice and Guidance Notes, CIPFA, January 2015

Managing the Business Risk of Fraud: A Practical Guide, Association of Certified Fraud Examiners and Institute of Internal Auditors, June 2008

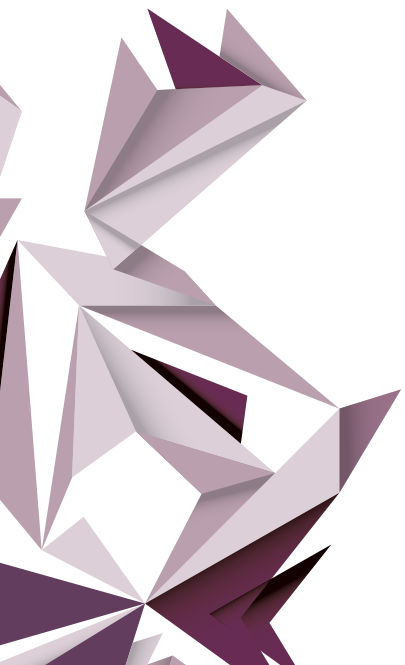
Managing Fraud Risk: The Audit Committee Perspective, Grant Thornton

Whistleblowing in the Public Sector: A good practice guide for workers and employers, NIAO and public audit agencies, November 2014



Published and printed by CDS

CDS 143426



ISBN 978-1-911003-06-9