

FRAUD POLICY

(including Anti-Fraud)

Document Title	Date of Previous Review	Date of Review	Responsibility of	Due date of next review
Fraud Policy	December 2022	January 2026	Patrick McKeown	January 2029
Date Approved at Strategic Group Meeting	2 February 2026			

RECORD OF CHANGES

Modifications made since the last review:

Record of Changes			
Reference Point	Change Comment	Date of Change	Initials
1.2	Change: zero tolerance rate in relation to fraud to zero tolerance approach toward fraud	30/01/206	SMcS
2.1	Change: the term is used to describe to the term FRAUD includes actions	30/01/206	SMcS
2.2	Remove: Obviously	30/01/206	SMcS
3.1	Change Annex 4.7 to Annex 4.9 Addition: to last bullet point – and with follow up information as soon as it becomes available.	30/01/206	SMcS
3.2	Change: line management and staff to all college staff	30/01/206	SMcS
4.2	Addition: Reporting any identified weaknesses or control failures promptly and implementing timely remedial actions where deficiencies are found.	30/01/206	SMcS
5.1	Addition: Every member of staff have a duty to ensure that public funds are safeguarded and	30/01/206	SMcS
5.3	Change: Procurement Officer to Head of Finance Addition: and Hospitality	30/01/206	SMcS
5.4	Remove: College has developed a Change: Further advice on the matter can be taken from 'Protect' (telephone 020 7404 6609, website protect advice.org.uk to Further advice on the matter can be taken from 'Protect' (telephone 020 3117 2520, website Protect - Speak up stop harm - Whistleblowing Homepage)	30/01/206	SMcS
7.3	Change: Repsonse to Response	30/01/206	SMcS
10	Change Annex 4.7.9 to Annex 4.9.10	30/01/206	SMcS
12	Remove: Corporate fraud risk that apply across the sector will be highlighted by Norther Ireland Finance Officers Network (NIFON) to ensure consistency.	30/01/206	SMcS
13	Addition: Senior	30/01/206	SMcS
Appendix 2	Addition: Requests to changes bank details Ransomware Bank Account hacking	30/01/206	SMcS
Appendix 3	Addition: Effective contracts management for supply of goods and services. - Stored securely - - Adherence to authorisation limits Remove: Rotate Staff - Fraud awareness training for all staff	30/01/206	SMcS
Appendix 4	Remove: This document was previously released as DAO (DoF 14/06)	30/01/206	SMcS
Appendix 5	Change: Head of Internal Audit to Risk Management Committee	30/01/206	SMcS
Appendix 6	Remove: Head of Division/Branch Change Director of Corporate services Division to Department for the Economy Change: Head of Branch to Head of Department Addition: Fraud Officer	30/01/206	SMcS

POLICY STATEMENT

The College will provide this policy in alternative formats on request where reasonably practicable, eg, Braille, Large Print, Computer Disk, Audio formats, etc, and/or alternative language.

The College is committed to promoting equality of opportunity and good relations in accordance with Section 75 of the Northern Ireland Act 1998. This policy should be interpreted in a manner consistent with the aforementioned legislation.

1 INTRODUCTION

- 1.1 There is a continuing need to raise staff awareness of their responsibility to safeguard public resources against the risk of fraud.
- 1.2 The North West Regional College (NWRC) has a **zero tolerance approach towards** fraud and is resolved to take all practical steps to eradicate it. NWRC requires all staff, at all times, to act honestly and with integrity and to safeguard the public resources for which they are responsible. Fraud is an ever-present threat to these resources and hence must be a concern to all members of staff. It is the policy of NWRC to identify and promptly investigate any possibility of fraudulent or related dishonest activities and when appropriate to pursue legal remedies available under the law.

This policy should be read in conjunction with the Public Interest Disclosure ('Raising Concerns') Policy. This policy allows employees who have suspicions of, or concern about, possible or actual malpractice to confidentially raise their concerns.

- 1.3 In circumstances where legal advice in relation to the handling of fraud has been sought from outside NWRC, the legal advisers should be apprised of the contents of the Fraud Policy and Fraud Response Plan and with relevant guidance issued by the Department of Finance, DfE and the NIAO. (Refer to the documents 'Managing the Risk of Fraud – A Guide for Managers (DAO (DFP) 06/11)', Annex 4.9 of Managing Public Money NI and Section 4.7 'Fraud' of the Financial Memorandum).
- 1.4 The purpose of this policy is to:
 - provide a definition of fraud;
 - set out responsibilities for fraud prevention and detection;
 - Set out procedures for reporting suspected and proven cases of fraud; and
 - set out responsibilities for the investigation of suspected fraud and the prosecution of offenders.

2 DEFINITION

2.1 Fraud is when someone obtains financial advantage or causes loss by implicit or explicit deception.

In law there is no specific offence of fraud: many of the offences referred to as fraud are covered by the Theft Acts. The term FRAUD includes actions such as deception, bribery, forgery, extortion, corruption, theft, embezzlement, misappropriation, false representation, concealment of material facts and collusion. For practical purposes fraud may be defined as the use of deception with the intention of obtaining an advantage, avoiding an obligation or causing loss to another party.

The Fraud Act 2006 came into effect on 15th January 2007. The Act states that fraud can be committed in three ways:

- False representation
- Failure to disclose information where there is a legal duty to disclose
- Abuse of position

2.2 Persons outside as well as inside NWRC can perpetrate fraud.

2.3 Four basic elements are necessary for a fraud to occur:

- People to carry out the fraud. They may be individuals within the organisation, outside the organisation, or a group of people working inside or outside the organisation.
- Assets to acquire fraudulently;
- Intent to commit the fraud;
- Opportunity.

Fraud can also be committed through the alteration, concealment or destruction of manual/computer records, the misuse of computer facilities, computer programmes and the Internet. The suspicion that any of these acts has taken place should be regarded as potentially fraudulent and dealt with as such.

2.4 Managers must ensure that the opportunities for fraud are minimised. Opportunities to commit fraud may be reduced by ensuring that a sound system of internal control, proportional to risk, has been established and that it is functioning as intended.

2.5 The UK Bribery 2010 came into effect on 1 July 2011. The act modernises the law on bribery and seeks to provide a revised framework of offences to combat bribery in the public and private sectors. It abolishes the offences of bribery at common law and the statutory offences in the Public Bodies Corrupt Practices Act 1889 and the Prevention of Corruption Act 1906.

3 NWRC'S RESPONSIBILITIES

3.1 The College's responsibilities regarding Fraud and Risk are as set out in Section 4.7 of the Management Statement and Financial Memorandum and Annex 4.9 of Managing Public Money in Northern Ireland, namely:

- the College should develop and maintain effective controls to prevent fraud and to ensure that, if it does occur, it will be detected without delay;
- the College must carry out vigorous and prompt investigation if fraud occurs and treat all fraud cases involving staff as gross misconduct;
- the College should take the appropriate legal and/or disciplinary actions in all cases against perpetrators of fraud;
- the College's investigation should consider, as a matter of course, whether there has been a failure of management/supervision and appropriate disciplinary action should be taken where failures have occurred;
- the Department (DfE) must be informed immediately of all cases of fraud or suspected fraud which are discovered and with follow up information as soon as it becomes available.

3.2 Although NWRC's Principal & Chief Executive, as delegated Accounting Officer, bears overall responsibility and is liable to be called to account for specific failures, these responsibilities fall directly on all college staff. All suspected frauds will be reported to the College's Audit & Risk Committee.

4 LINE MANAGERS' RESPONSIBILITIES

4.1 The responsibility for the prevention and detection of fraud rests primarily with management. Line managers should, therefore, be familiar with the risks involved within their areas of responsibility and for ensuring that an adequate system of internal control exists and is operating effectively.

4.2 Managers are responsible for:

- regularly reviewing and testing control systems for which they are responsible;
- ensuring that controls are being complied with;
- satisfying themselves that their systems continue to operate effectively.

- Reporting any identified weaknesses or control failures promptly and implementing timely remedial actions where deficiencies are found.
- 4.3 In terms of establishing and maintaining effective controls it is generally desirable that:
- staff are properly trained in how to deal with fraud risks;
 - staff working in areas where there is a higher risk of fraud (eg Finance areas) have a thorough understanding of the DoF guide on 'Managing the Risk of Fraud'.
 - if possible, there is rotation of staff, particularly in key posts;
 - wherever possible, there is some segregation of duties so that control of a key function(s) and tasks are not vested in one individual;
 - supervision should be greater in any work area where segregation of duties and rotation of staff is not practical;
 - the Board of Governors and Management have established adequate and efficient systems of internal financial and management control.

5 STAFF RESPONSIBILITIES

- 5.1 Every member of staff have a duty to ensure that public funds are safeguarded and should alert their line manager where they believe the opportunity for fraud exists. It is the responsibility of every member of staff to report details immediately to their line manager if they suspect that a fraud has been committed or if they see any suspicious acts or events. The Line Manager should inform the Fraud Officer immediately. However, if line management involvement is suspected, the matter should be raised with the next senior officer or the Principal and Chief Executive who should inform the Fraud Officer (Finance Director).
- 5.2 Staff should also assist in any investigations by making available all relevant information and by co-operating in interviews. Any information provided by staff will be treated confidentially.
- 5.3 All College staff should be conscious of conducting themselves in accordance with the principles on Public Life (known as the 'Nolan Principles') which are Selflessness, Integrity, Objectivity, Accountability, Openness, Honesty and Leadership.

As stewards of public funds, NWRC staff must have, and be seen to have, high standards of personal integrity. Staff should not accept inducements from a third party which might be seen to compromise

their integrity and should declare any potential conflicts of interest. Any gifts etc over the value of £50 which are received should be recorded in a Register of interests kept by the Head of Finance. (See Gifts and Hospitality Policy)

- 5.4 It is also essential that staff understand, and adhere, to laid down systems and procedures, including those of a personnel/management nature such as submission of expenses claims and records of absence, flexi and annual leave.

The Public Interest Disclosure (Northern Ireland) Order 1998 is designed to encourage employees to disclose information about alleged wrongdoing in defined circumstances. The Order protects 'whistleblowers' that make responsible disclosures from dismissal and victimisation. The 'Raising Concerns Policy' sets out the procedures and protections which will apply to staff making such disclosures. Further advice on the matter can be taken from 'Protect' (telephone 020 3117 2520, website [Protect - Speak up stop harm - Whistleblowing Homepage](#))

6 INTERNAL AUDIT

- 6.1 Internal Audit is responsible for the provision of an independent and objective opinion to the Accounting Officer on risk management, control and governance. The adequacy of arrangements for managing the risk of fraud and ensuring the College promotes an anti-fraud culture is a fundamental element in arriving at an overall opinion.
- 6.2 Internal Audit has no responsibility for the prevention or detection of fraud. However, internal auditors are alert in all their work to risks and exposures that could allow fraud. Individual audit assignments, therefore, are planned and prioritised to assist in deterring and preventing fraud by examining and evaluating the effectiveness of control commensurate with the extent of the potential exposure/risk.
- 6.3 Internal Audit is available to offer advice and assistance on risk management/internal control issues, as well as advice and assistance in relation to cases of fraud or suspected fraud. The Finance Director will report all cases of suspected or actual fraud to Internal Audit as deemed appropriate.

7 INVESTIGATIONS

- 7.1 It is NWRC's policy that there will be consistent handling of all suspected fraud cases without regard to position held or length of service. As a matter of course, supervisory negligence will be considered as part of any investigation.

- 7.2 Investigators should have free access to all staff, records and premises in order to carry out investigations.
- 7.3 If there is suspicion of fraud, prompt action is essential, and all cases of suspected or actual fraud should be reported immediately to the Finance Director (Patrick McKeown, patrick.mckeown@nwrc.ac.uk, +44 02871278759) who will in turn notify DfE Fraud & Raising Concerns Branch. Preliminary enquiries should be undertaken until any suspicion has been reported to the Finance Director. As detailed in the Fraud Response Plan, it is imperative that enquiries should not prejudice subsequent investigations or corrupt evidence, therefore, if in doubt ask for advice.
- 7.4 If an initial investigation confirms the suspicion that a fraud has been perpetrated or attempted, management should follow the guidance provided in the Fraud Response Plan. The Fraud Officer should consult with the HR Manager if it's believed that a staff member is or has been involved in the fraud or suspected fraud.

8 DfE Fraud & Raising Concerns Branch (FRCB)

- 8.1 On behalf of the department and all Arm's Length Bodies (ALBs), FRCB maintains a management information system for all notified fraud / suspected fraud allegations. Per the requirements of Managing Public Money Northern Ireland (MPMNI), they report all instances to the Northern Ireland Audit Office and the Department of Finance. The branch also provides oversight and monitoring of all cases, advice and guidance and updates to managers and the Departmental Audit and Risk Assurance Committee.

9 DISCIPLINARY ACTION

- 9.1 After full investigation, NWRC will take legal and/or disciplinary action in all cases where it is considered appropriate.
- 9.2 Where supervisory negligence is found to be a contributory factor, disciplinary action should also be initiated against those managers/supervisors responsible. In certain circumstances it can be an offence under Section 5 of the Criminal Law Act (Northern Ireland) 1967 not to report certain offences to the police (PSNI).
- 9.3 The College will consider informing the PSNI after considering the specific details of the fraud – for example, value, potential for further fraud or misappropriation.
- 9.4 NWRC's Disciplinary Procedures and Code of Conduct provide guidance on conduct and disciplinary procedures. Compliance with this Fraud Policy is compulsory and failure to do so may result in disciplinary action.

- 9.5 Losses resulting from fraud should be recovered, subject to the policy on write-offs, if necessary, through civil action.
- 9.6 Where an employee misappropriates or steals money collected from the public, the College will act on the principle that an employer is liable for torts committed by the employee within the scope of his/her employment.

10 ANNUAL FRAUD RETURN

Managing Public Money NI Annex 4.9.10 requires the College to submit an annual return to DfE (which is updated and submitted quarterly) giving details of all discovered cases of suspected and proven fraud (including attempted fraud). A record of cases will be maintained by the Finance Director.

11 NATIONAL FRAUD INITIATIVE

The National Fraud Initiative (NFI) is an effective data matching exercise. It compares information held by different organisations and within different parts of an organisation to identify potentially fraudulent claims and overpayments. The Comptroller and Auditor General for Northern Ireland can undertake data matching exercises, requesting data from a range of public bodies, for the purposes of assisting in the prevention and detection of fraud.

The College participates in the NFI exercise providing payroll and trade creditor data sets to successfully identify cases of suspected fraud and overpayment. Continued participation in the NFI represents a key strand of the College's anti-fraud policy.

12 FRAUD RISK ASSESSMENTS

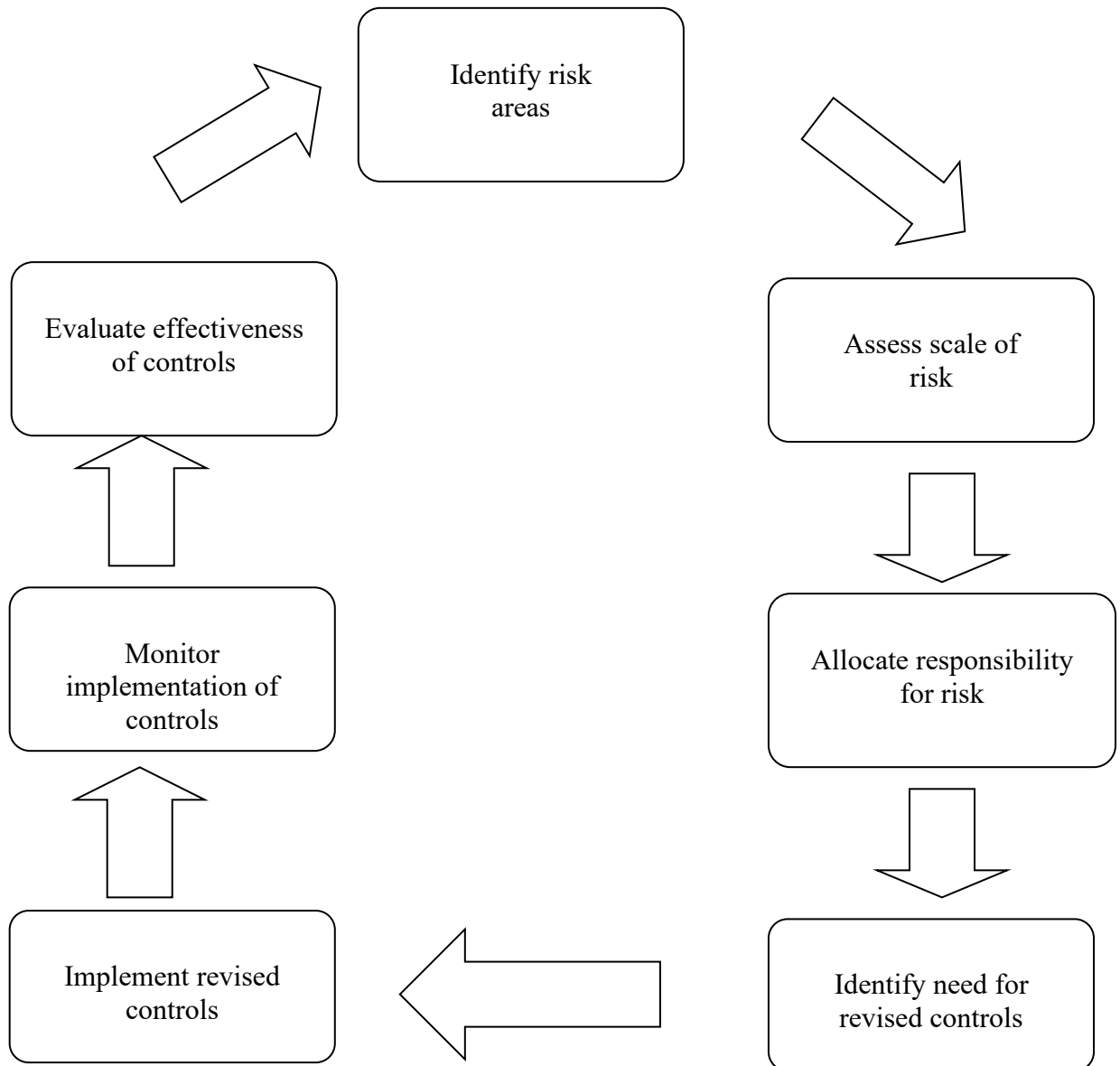
A major element of good corporate governance is a sound assessment of the organisation's business risks. The key to managing the risk of fraud is the same in principle as managing any other business risk and should be approached systematically at both the organisational and the operational level. The assessment of risk should be part of a continuous cycle rather than a one-off event: as systems and the environment change, so do the risks to which departments will be exposed. **Figure 1** below sets out the key stages of a risk management cycle to help deal with fraud. Internal Audit is available to offer advice and assistance on risk management/internal control issues along with Department for the Economy's Fraud and Raising Concerns Branch.

In addition, **Appendix 5** provides Guidance on Performing an Assessment of Fraud Risks.

Fraud risk assessments should be reviewed every 2 year(s) or when there is significant organisational change, to ensure that any new fraud risks are identified and addressed.

The Audit and Risk Committee should be involved in reviewing and challenging the corporate fraud risk assessment and control environment and reporting on this to the Governing Body for its consideration. Governing Body oversight at times of significant change is particularly important.

Figure 1: RISK ASSESSMENT CYCLE



13. CONCLUSION

It is appreciated that the circumstances of individual irregularities and/or frauds will vary, but it is important that all are vigorously and promptly investigated and that appropriate remedial action is taken. Management should be conscious of their responsibility to protect public funds and, as such, should always be alert to the potential for fraud.

Any queries in connection with this policy should be made to the Fraud Officer (Finance Director).

The Board of Governors and Senior Management will always seek legal advice before deciding on a course of action.

APPENDIX 1

INDICATORS OF FRAUD

- Missing expenditure vouchers and unavailable official records
- Crisis management coupled with a pressured business climate
- Profitability declining
- Excessive variations to budgets or contracts
- Refusals to produce files, minutes or other records
- Related party transactions
- Increased employee absences
- Borrowing from fellow employees
- An easily led personality
- Covering up inefficiencies
- Lack of Board oversight
- No supervision
- Staff turnover is excessive
- Figures, trends or results which do not accord with expectations
- Bank reconciliations are not maintained or can't be balanced
- Excessive movement of cash funds
- Multiple cash collection points
- Remote locations
- Unauthorised changes to systems or work practices
- Employees with outside business interests or other jobs
- Large outstanding bad or doubtful debts
- Offices with excessively flamboyant characteristics
- Employees suffering financial hardships
- Placing undated/post-dated personal cheques in petty cash
- Employees apparently living beyond their means
- Heavy gambling debts
- Signs of drinking or drug abuse problems
- Conflicts of interest
- Lowest tenders or quotes passed over with scant explanations recorded
- Employees with an apparently excessive work situation for their position
- Managers bypassing subordinates
- Subordinates bypassing managers
- Excessive generosity
- Large sums of unclaimed money
- Large sums held in petty cash
- Lack of clear financial delegations
- Secretiveness
- Apparent personal problems
- Marked character changes
- Excessive ambition
- Apparent lack of ambition

INDICATORS OF FRAUD (CONTINUED)

- Poor morale
- Excessive control of all records by one officer
- Poor security checking processes over staff being hired
- Unusual working hours on a regular basis
- Refusal to comply with normal rules and practices
- Personal creditors appearing at the workplace
- Non taking of leave
- Excessive overtime
- Large backlogs in high-risk areas
- Lost assets
- Unwarranted organisation structure
- Absence of controls and audit trails
- Socialising with clients – meals, drinks, holidays
- Seeking work for clients
- Favourable treatment of clients – eg allocation of work
- Altering contract specifications
- Contract not completed to specification
- Contractor paid for work not done
- Grants not used for specified purpose – eg Leasing capital equipment instead of purchasing them

Corporate Fraud

- Lack of thorough investigations of alleged wrongdoing
- Pecuniary gain to organisation – but no personal gain

APPENDIX 2

COMMON METHODS AND TYPES OF FRAUD

- Payment for work not performed
- Claiming for overtime not worked
- Secondary employment during working hours
- Abuse of flexi
- Working while on sick leave
- Over claiming travel and expenses
- Running a private business with official assets, for example, departmental telephone and IT systems
- Forged endorsements
- Altering amounts and details on documents
- Collusive bidding
- Overcharging
- Writing off recoverable assets or debts
- Unauthorised transactions
- Selling information
- Cheques made out to false persons
- False persons on payroll
- Theft of official purchasing authorities such as order books
- Unrecorded transactions
- Transactions (expenditure/receipts/deposits) recorded for incorrect sums
- Ransomware
- False official identification used
- Damaging/destroying documentation
- Using copies of records and receipts
- Using imaging and desktop publishing technology to produce apparent original invoices
- Charging incorrect amounts with amounts stolen
- Transferring amounts between accounts frequently
- Delayed terminations from payroll
- Bribes
- Skimming odd pence and rounding
- Using facsimile signatures
- False compensation and insurance claims
- Stealing of discounts
- Selling waste and scrap
- Altering stock records
- Altering sales records
- Cash stolen
- Supplies not recorded at all
- Stolen equipment and supplies
- Requests to change bank details
- Bank Account hacking

APPENDIX 3

EXAMPLES OF GOOD MANAGEMENT PRACTICES WHICH MAY ASSIST IN COMBATING FRAUD

- All income is promptly entered in the accounting records with the immediate endorsement of all cheques
- Regulations governing contracts and the supply of goods and services are properly enforced
- Effective contracts management for supply of goods and services
- Accounting records provide a reliable basis for the preparation of financial statements
- Controls operate which ensure that errors and irregularities become apparent during the processing of accounting information
- A strong internal audit presence
- Management encourages sound working practices
- All assets are properly recorded, stored securely and provision is made known for expected losses
- Accounting instructions and financial regulations are available to all staff and are kept up to date
- Effective segregation of duties exists, particularly in financial accounting and cash/securities handling areas
- Close relatives do not work together, particularly in financial, accounting and cash/securities handling areas
- Act immediately on internal/external auditor's report to rectify control weaknesses
- Review, where possible, the financial risks of employees
- Issue accounts payable promptly and follow-up any non-payments
- Set standards of conduct for suppliers and contractors
- Maintain effective security of physical assets; accountable documents (such as cheque books, order books); information, payment and purchasing systems
- Review large and unusual payments
- Perpetrators should be suspended from duties pending investigation

- Proven perpetrators should be dismissed without a reference and prosecuted
- Query mutilation of cheque stubs or cancelled cheques
- Store cheque stubs in numerical order
- Adherence to authorisation limits
- Undertake test checks and institute confirmation procedures
- Develop well defined procedures for reporting fraud, investigating fraud and dealing with perpetrators
- Maintain good physical security of all premises
- Randomly change security locks and rotate shifts at times (if feasible and economical)
- Conduct regular staff appraisals
- Review work practices open to collusion or manipulation
- Develop and routinely review and reset data processing controls
- Regularly review accounting and administrative controls
- Set achievable targets and budgets, and stringently review results
- Ensure staff take regular leave
- Ensure all expenditure is authorised
- Conduct periodic analytical reviews to highlight variations to norms
- Take swift and decisive action on all fraud situations
- Ensure staff are fully aware of their rights and obligations in all matters concerned with fraud

REFERRAL TO PSNI: ACCEPTANCE CRITERIA

1. These criteria set out the conditions necessary for a suspected fraud case to be referred to the PSNI. **However, the decision to accept a case for investigation rests fully with the PSNI who will provide their decision in writing.**
 - It must be established that there are reasonable grounds to believe that a criminal offence has been committed.
 - Deliberate criminal intent needs to be clearly defined. The fraud needs to be more than an error or omission.
 - The allegations should concern recent events and should not have become stale by reason of age. Incidents, which are over two years old before discovery, need to be judged individually on their merits, including availability of documentary evidence and the reliability of witness evidence.
 - To comply with the rules governing disclosure, the department/body will identify and preserve all original documents and other exhibits relating to any intended complaint.
 - The department/body should be prepared to supply all original relevant documents and exhibits to the police if an investigation is accepted and commenced. Such evidential material should be securely held, in accordance with PACE provisions, before formal hand over to the PSNI.

Appendix 4 (continued)

PSNI AGREED FORMAT OF EVIDENCE PACK

1. Evidential packages should contain a detailed summary of all relevant information surrounding the allegations made. This should include the nature of the allegations against the suspect, including the full name, address and date of birth of the suspect.

2. The package should also include: -
 - All available details of any other parties suspected of involvement in the alleged fraud, including the reasons for the suspicions;

 - A brief summary of the allegations including estimated values of alleged crime and relevant dates;

 - A full description of the nature of the crime and the circumstances surrounding it. This should include full details of any investigations already undertaken by the department/body or anyone acting on their behalf;

 - Copies of all relevant documents, each individually numbered and identified in the summary;

 - Copies of all statements obtained from suspects;

 - Names and addresses of all witnesses identified at the time of reporting to the police, including copies of any statements;

 - Any police reference numbers, which may already apply to any part of the case; and

 - A name and contact point.

Appendix 5

GUIDANCE ON PERFORMING AN ASSESSMENT OF FRAUD RISKS

This appendix provides guidance on how to perform an assessment of fraud risks using the template provided below.

Business Area:		<i>[Insert name of business area]</i>				
Fraud Risk Assessment of:		<i>[Insert a description of the area being assessed eg branch, process, type and value of transactions, nature of expenditure, any risks realised, any internal audit or external audit recommendations or concerns.]</i>				
Assessment completed by:		<i>[Insert name of officer completing the assessment]</i>				
Assessment reviewed and agreed by:		<i>[Insert name of line manager reviewing and agreeing the assessment]</i>				
Assessment agreed on:		<i>[Insert date assessment is agreed]</i>				
Next assessment due on:		<i>[Insert date for completion of next fraud assessment]</i>				
1	2	3	4	5	6	7
FRAUD RISK	IMPACT (H, M, L)	LIKELIHOOD (H, M, L)	KEY CONTROLS	RESIDUAL RISKS	PLANNED ACTION	ACTION TAKEN

How to complete the assessment

1. Identify the key fraud risks facing your business and detail these in **Column 1**.

Examples might be:

- fraudulent subsidy/grant claims;
- payment made on false documentation;
- theft of assets;
- misappropriation of cash;
- false accounting;
- contract fraud;
- procurement fraud;
- collusion;
- computer fraud;
- fraudulent encashment of payable instruments;
- travel and subsistence fraud;
- false claims for hours worked;
- bribery.

2. Assess the impact of the identified fraud risk should it occur – High, Medium or Low (**Column 2**). What damage could be done in relation to achievement of objectives, financial loss, reputation etc?
3. Assess the likelihood of the identified fraud risk occurring – High, Medium or Low (**Column 3**). High would be probable/likely, low would be improbable/unlikely.
4. Identify the key controls already in place to address each identified risk (**Column 4**);

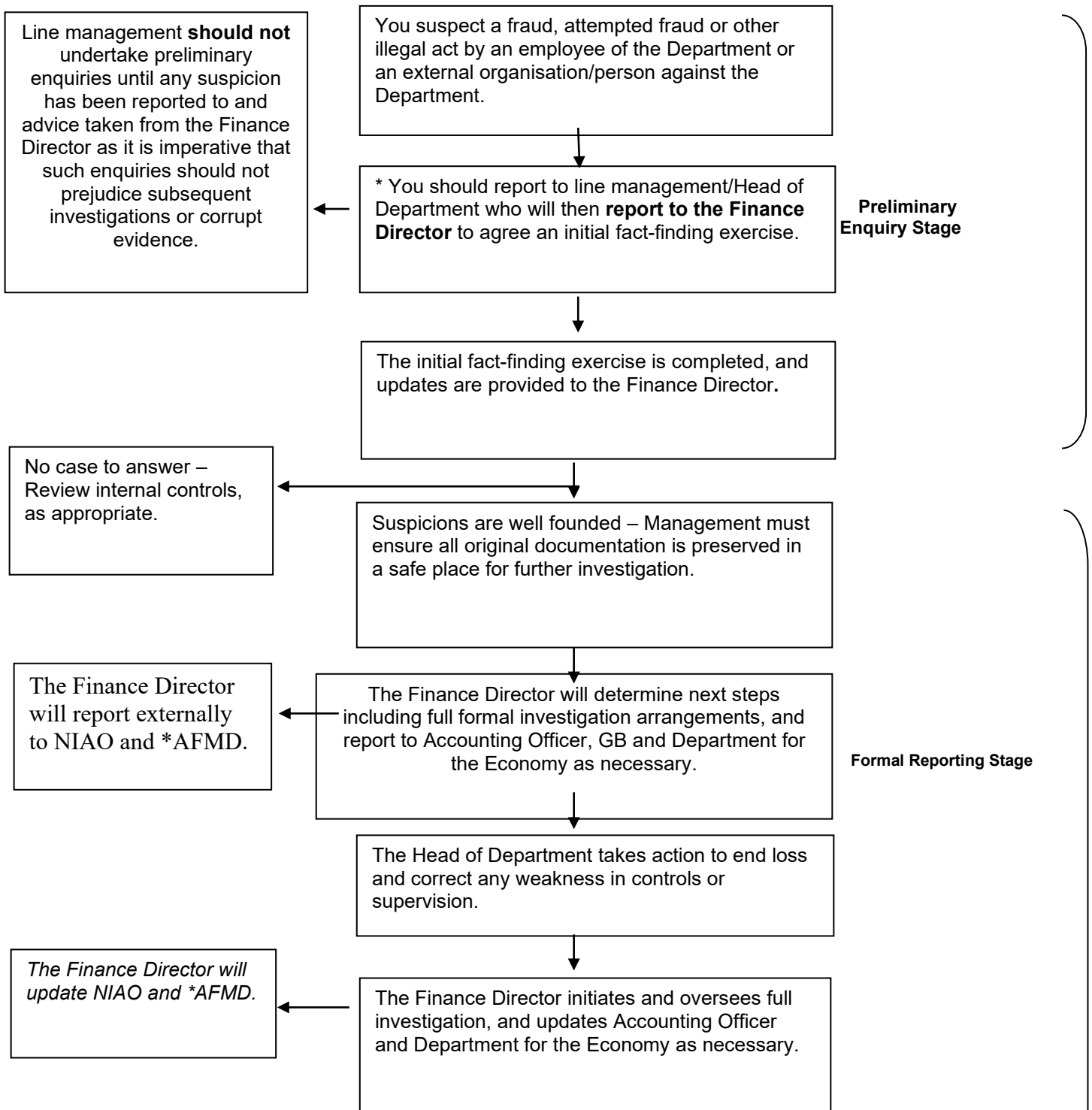
Appendix 5 (continued)

Examples might be:

- segregation of duties
- payment authorisation levels
- payment/lodgement reconciliations
- management checks and reviews
- tendering process
- transparent approval process
- inter-system checks
- physical controls such as safes, key safes etc.
- logical access controls
- physical access controls
- asset register and inventory checks
- audit logs
- project monitoring
- performance monitoring
- independent/unannounced inspections
- post-payment checks
- training
- manuals
- staff rotation
- irregularity recording, investigation and reporting process etc.

5. Determine if any risk still exists after the application of the identified controls (**Column 5**). For example, the original risk detailed in column 1 will probably still be a risk post-control although the effective application of the controls detailed in column 4 will reduce the likelihood of occurrence.
6. Detail in **Column 6** what further action you are going to take to address the residual risk. It may be that control over the risk lies elsewhere and as a consequence you will have to accept the risk. If this is the case, justify why you are accepting the risk.
7. If you are planning further action to treat the risk, state what this is, who will be responsible for the action and when it is to be implemented.
8. **Column 7** will be used by you for internal reviews of the risk management framework.
9. Issue completed framework to the Risk Management Committee annually. Review internally on a regular basis – at least every 6 months.

FLOWCHART OF KEY ACTIONS



**Accountability and Financial Management Division*

* If you are concerned that line management may be involved in a suspected or actual fraud, you should report it to the next appropriate level, i.e. Head of Department or Director. Alternatively, at any stage in the process, you can contact the Fraud Officer (Finance Director). You can also contact *Public Concern at Work*.