TNI Anti-Fraud & Bribery Policy

Contents

1. Policy Aims

TNI is committed to the prevention of fraud, bribery and other irregularities and the promotion of an anti-fraud culture.

TNI operates a **zero-tolerance attitude** to fraud and corruption, whether from internal or external sources. The TNI requires staff and individuals/organisations that it deals with, to act with honesty and integrity, to safeguard the public resources and to report all suspicions of fraud and corruption. This policy is concerned with both internal and external fraud committed against TNI and applies to Board Members, Directors and all staff (including full time, part time, temporary, casual and agency staff).

Every case of attempted, suspected or proven fraud will be thoroughly investigated and where appropriate, referred to the Police Service of Northern Ireland (PSNI). TNI will also seek to recover any loss suffered through fraud and if appropriate, will take civil, criminal and/or disciplinary action.

TNI encourages anyone having reasonable suspicions of fraud or bribery to report them in accordance with the fraud and bribery response plan, or the TNI Whistleblowing policy. It is also TNI policy that no one will suffer in any way as a result of reporting a reasonably held suspicion. For these purposes "reasonably held suspicions" shall mean any suspicion that is believed by the individual to be true, and which is raised in good faith.

TNI promotes an anti-fraud and anti-bribery culture by encouraging management to create conditions in which staff members have neither the motivation, nor the opportunity to commit fraud or either offer or accept bribes. Managers have prime responsibility for establishing internal control arrangements to minimise the risk of fraud, corruption and other irregularities within their business areas as the first line of defence against these issues, supported by the establishment and maintenance of carefully designed and consistently operated procedures.

In line with their responsibilities, the Chief Executive and Director of Finance shall monitor and ensure compliance with directions issued by the Department of Finance and Department for the Economy on fraud and corruption.

All cases of suspected fraud or bribery in TNI must be reported to the DFE as outlined in this policy. The Department will then report these suspected frauds to the Northern Ireland Audit Office (NIAO) and the Department of Finance (DoF). This should only be done by the Department.

This policy along with the associated Response Plan, which is an integral part of this policy, which prescribes what staff members should do if they suspect fraud, bribery or other wrongdoing, in any business associated with TNI.

2. What is Fraud and what are its impacts?

In essence, fraud is a deliberate act by an individual or group of individuals and is therefore always intentional and dishonest.

The key legislation which may be used to prosecute fraud is the Fraud Act 2006 and supplements other legislation, such the Theft Act (NI) 1969 and the Theft (NI) Order1978. The Fraud Act 2006 became law in Northern Ireland in January 2007 and created a new general offence of fraud which can be committed in three ways:

a. **Fraud by false representation;**

   If an individual dishonestly makes a false representation and intends by making the representation to make a gain for himself or another, or to cause loss to another or expose another to risk of loss. A representation is false if it is untrue or misleading, and the person making it knows that it is, or might be, untrue or misleading.

b. **Fraud by failing to disclose information**

   If an individual dishonestly fails to disclose to another person information which he is under a legal duty to disclose and intends, by failing to disclose the information, to make a gain for himself or another, or to cause loss to another or expose another to risk of loss.

c. **Fraud by abuse of position**

   If an individual occupies a position in which he is expected to safeguard, or not to act against, the financial interests of another person, and he dishonestly abuses that position, and intends,

by means of the abuse of that position, to make a gain for himself or another, or to cause loss to another or to expose another to a risk of loss.

It also established a number of specific offences to assist in the fight against fraud. These include an offence of possessing articles for use in fraud and an offence of making or supplying articles for use in fraud.

For the purposes of this document, fraud covers any deception which harms TNI's interests. It may involve:

- manipulation, falsification or alteration of records or documents;
- suppression or omission of the effects of transactions from records or documents;
- recording of transactions without substance;
- misappropriation (theft) or wilful destruction or loss of assets including cash;
- deliberate misapplication of accounting or other regulations or policies;
- bribery and corruption;
- deception and collusion;
- money laundering; and
- computer fraud, for example fraud in which IT equipment is used to manipulate computer programmes or data dishonestly, or where the existence of an IT system was a material factor in the perpetration of the fraud.

3. What is Bribery and what are the impacts?

The Bribery Act 2010 came into force on the 1st July 2012 and was intended to provide a stricter definition of bribery than was provided in the Fraud Act 2006 and other legislation. The legislation creates the following four statutory offences:

(1). The general offence of offering, promising or giving a bribe;
(2). The general offence of requesting, agreeing to receive, or accept a bribe;
(3). The offence of bribing a foreign public official to obtain or retain business; and
(4). A new corporate offence of failing to prevent bribery.

The first three offences listed above relate to the individual and make it a criminal offence to give or receive a bribe. The consequences of an individual being convicted of any of the first three offences above can involve a prison sentence of up to 10 years and personal liability for senior officers of the organisation, in relation to the corporate offence of failing to prevent bribery.

The fourth offence above relates to the offence committed when a corporate body fails to take the necessary measures to prevent bribery on their behalf. This includes staff, or other third parties, such as a contractor, an agent, or a service provider irrespective if it is for charitable or educational aims or purely public functions.

4. When fraud or bribery is suspected or detected

Staff members are advised to report any suspicions of fraud or bribery urgently as per the Fraud and Bribery Response Plan (Section B). The plan forms part of this policy and should be read in conjunction with it.

The Fraud and Bribery Response Plan outlines TNI's procedures for responding to any incidents of suspected fraud, bribery or other irregularity . The Response Plan sets out how suspicions should be raised and how investigations will be conducted and concluded.

All matters will be dealt with in confidence and if appropriate, in strict accordance with the terms of the Public Interest Disclosure (Northern Ireland) Order 1998. This statute protects the legitimate personal interests of staff. Vigorous and prompt investigations will be carried out into all cases where suspected fraud is discovered or reported.

5. Responsibilities

a) Chief Executive

The Chief Executive as Accounting Officer is responsible for ensuring the establishment and maintenance of a sound system of internal controls, designed to respond to and manage the whole

range of risks that the organisation faces. In broad terms, managing the risk of fraud and bribery involves:

- assessing the organisation's overall vulnerability to fraud and bribery;
- identifying the areas most vulnerable to fraud risk and bribery risk;
- evaluating the scale of risk associated with fraud and bribery and responding to those risks;
- measuring the effectiveness of the fraud / bribery risk strategies;
- reporting suspected cases of fraud and bribery to the DfE; and
- Regularly reviewing the TNI's Anti-Fraud and Bribery Policy, and associated the Response Plan, and ensure compliance with the policy.

b) Directors and Heads of Functions

The Directors and Heads of Service are responsible for:

- Dealing swiftly and firmly with those who defraud TNI or who are found to be corrupt after an investigation under the Fraud Response Plan.
- Carrying out reviews of risks in the areas under their responsibility and work with the Director of Finance and Auditors to improve controls.
- Ensuring that responsibilities for controls are clearly assigned to reporting staff.

c) Director of Finance

The Director of Finance has delegated responsibility for managing the risk of fraud at an organisational level. The Director of Finance's responsibilities include:

- developing a fraud risk profile and undertaking a regular review of the fraud risks;
- designing an effective control environment to prevent fraud, bribery and other irregularities;
- establishing a well-publicised, Anti- Fraud and Anti Bribery Policy and appropriate mechanisms for staff and members of the public to report their suspicions of fraud.
- report to the Senior Management Team, Board and Audit Committee on all aspects of fraud risk management.
- ensuring that appropriate anti-fraud training is available to appropriate staff in order to meet the defined competency levels;
- ensuring and overseeing that vigorous and prompt investigations are carried out if fraud occurs or is suspected;

- ensuring that appropriate disciplinary action is taken where appropriate, including against individuals failing to comply with controls or the reporting of suspected fraud; and
- ensuring that appropriate action is taken to recover assets and to minimise the risk of similar frauds occurring in future.

d) Operational Managers

All operational managers are responsible for preventing and detecting fraud. This includes:

- assessing the types of risk (including fraud risk) involved in the operations for which they are responsible. Each risk should be assessed in terms of likelihood and potential impact;
- ensuring that an adequate system of internal control exists within their areas of responsibility, including the identification of adequate and effective management controls for each risk identified;
- Ensuring that controls are being complied with and their systems continue to operate effectively;
- regularly reviewing and testing the control systems for which they are responsible;
- reviewing controls and implementing new controls to reduce the risk of similar fraud occurring where frauds have taken place;
- reassessing risks as a result of the introduction of new systems or amendments to existing systems;
- quantifying the occurrence of fraud on an annual basis and updating risk registers and control frameworks to reflect the quantum of fraud within the business area. Where appropriate, strategies should be devised to combat recurrence of fraud and targets set to reduce the level of fraud;
- promptly implementing recommendations of internal and external audit; and
- ensuring compliance with anti-fraud policies and the fraud response plan.

As fraud prevention is the ultimate aim, anti-fraud measures should be considered and incorporated in every system and programme at the design stage. Internal Audit will offer advice to managers on risk and control issues in respect of existing and developing systems / programmes.

e) All Staff Responsibilities

TNI staff must have, and be seen to have, high standards of personal integrity. It is also essential that staff understand, and adhere to, systems and procedures including those of a HR / management

nature such as submission of expenses claims and records of absence, flexi and annual leave and acceptance or provision of gifts and hospitality.

Every member of staff is responsible for:

- acting with propriety in the use of official resources and the handling and use of public funds.
- conducting themselves in accordance with the seven principles of public life set out in the first report of the Nolan Committee "Standards in Public Life" They are: selflessness, integrity, objectivity, accountability, openness, honesty and leadership;
- being alert to the possibility that unusual events or transactions could be indicators of fraud and alerting their line manager where they believe the opportunity for fraud exists (Annex 2: examples of indicators of fraud).
- Reporting details immediately through the appropriate channels if they suspect that a fraud has been committed;
- cooperating fully with whoever is conducting internal checks or reviews, or fraud investigations; and
- assisting Internal Audit, or their agents, in conducting fraud investigations. Staff must assist investigations by making available all relevant information and by co-operating in interviews. Any information provided by staff will be treated confidentially subject to Freedom of Information requirements and/or legal obligations.

f) Audit Committee

The Audit Committee will have oversight of this Policy and associated Fraud Response Plan. The Audit committee will:

- review the Anti-Fraud & Bribery Policy & Response Plan and consider whether it meets recommended practices;
- champion an anti-fraud culture throughout the TNI;
- review the fraud risk profile and estimate of fraud loss or potential harm to TNI.
- review the anti-fraud activity, seeking assurance that it is in line with the policy and response plan; and
- oversee any areas of fraud identified and monitor action plans to address control weaknesses.

g) Internal Audit

TNI's Internal Audit service is responsible for:

- reviewing the arrangements management have in place to prevent and detect fraud and other wrongdoing and ensuring that TNI promotes an anti-fraud culture;
- ensuring that management has reviewed its risk exposures and identified the possibility of fraud as a business risk;
- assisting management as required in undertaking investigations into allegations of fraud and corruption.
- assisting in the deterrence and prevention of fraud by examining and evaluating the effectiveness of controls.

6. Sanction and Redress

Staff suspected of involvement in fraudulent activity or acts pertaining to the Bribery Act 2010, may be subject to one or more of the following sanctions:

- disciplinary, with dismissal sought where the offence is considered to constitute 'gross misconduct';
- criminal, where the relevant law enforcement agency considers it to be in the public interest to pursue a prosecution;
- civil recovery of monies or assets fraudulently acquired; and
- professional debarment, whereby the TNI will make a referral to the employee's professional regulatory bodies where appropriate.

Each option should be carefully considered in order to ensure that the most appropriate course of action is taken. It is important that any civil or disciplinary action does not impair a criminal investigation and vice versa.

TNI will consider terminating contracts with any organisation which is convicted of the corporate offence of failing to prevent bribery and disbarring them from any future Tender exercises for TNI Contracts.

7. Prosecution

Where evidence suggests that a criminal offence has been committed, the Director of Finance will consult with the Chief Executive and DfE about a referral to PSNI.

TNI will liaise with the PSNI to ensure that any other action instigated under the Response Plan does not prejudice or interfere with criminal proceedings.

Where TNI staff members are required to liaise with the Police as potential witnesses in matters regarding the prosecution of fraud or bribery, TNI will provide all the support and assistance that may be required, or that the staff member feels that they may need in assisting the Police. This support does not extend to any employee or contractor who is subsequently charged with fraud or bribery related offences committed against TNI.

8. Recovery of Loss

Preventing further loss and recovery of any losses incurred are the primary objectives of any investigation. The Chief Executive shall ensure that in all investigations, the amount of any loss shall be quantified. Repayment of losses should be sought in all cases.

Where the loss is substantial, legal advice should be obtained without delay on the potential to freeze the suspect's assets through the court, pending conclusion of the investigation. Legal advice should also be obtained on the prospects for recovering losses through the civil courts, should the suspect refuse to repay the loss, TNI should seek to recover costs in addition to any losses.

9. Theft of Personal Property

While the theft of the personal property or cash of a member of staff does not constitute fraud against TNI, it is nevertheless essential that any such incidents are reported through line management so that appropriate action (such as notification of the police) can be taken.

Responsibility for the prevention of the theft of personal property or cash rests with individuals who are ultimately responsible for their own property. However, it is prudent for managers to remind staff not to leave personal valuables or cash unattended.

10. Conclusion

The circumstances of individual frauds and bribes will vary. TNI takes fraud and corruption extremely seriously and actively seeks to prevent any level of fraud or bribery. All cases of actual or suspected fraud or bribery will be vigorously and promptly investigated and appropriate action, including the recovery of assets wrongfully obtained, will be taken. Staff must report suspected fraud, bribery or other suspicious activity immediately.

Any queries in connection with this policy document should be directed to TNI's Director of Finance. TNI's Internal Audit provider is available to offer advice and assistance on risk management/internal control issues. This should be coordinated through the Director of Finance.

SECTION B: Fraud & Bribery Response Plan

1. Introduction

This plan describes TNI's intended response to a report of a suspected fraud or bribery. It provides guidance and procedures that allow for evidence gathering and collation in a manner that will facilitate informed initial decisions, whilst ensuring that evidence gathered will be admissible in any further criminal, civil or disciplinary action.

This guidance will require careful consideration in relation to the actual circumstances of each case before action is taken. The use of the plan should enable TNI to prevent loss of public money, recover losses and establish and secure the evidence necessary for any civil, criminal or disciplinary action.

The Response Plan complements the Anti-Fraud Policy and forms part of the overall Anti-Fraud & Bribery Strategy of TNI.

2. Reporting suspected or proven Fraud

When a member of staff suspects that a fraud, bribe, or other corruption has occurred, he/she must notify their line Manager immediately. If there is a concern about the line manager, then the matter should be reported to the next appropriate level. Alternatively, the Director of Finance should be contacted.

Speed is of the essence and this initial report should be verbal. If it is not appropriate for staff to raise their concerns with their line manager, the matter should be brought to the attention of Chief Executive or other senior staff as follows:

- Chief Executive.
- Director of Finance.
- Chair of TNI Audit & risk Assurance Committee.
- TNI's Internal Auditor.

If there is any suggestion that the Chief Executive Officer or Director of Finance is involved in the fraud, the Head of Internal Audit at DfE should be contacted in the first instance in conjunction with the Head of HR in TNI.

In notifying line management of suspected fraud, staff should be aware of the TNI's Whistleblowing Policy and the protection that this provides under the Public Interest Disclosure (Northern Ireland) Order 1998.

On verbal notification of a potential fraud or bribery, the line Manager shall contact the Director of Finance, who must immediately inform the DfE sponsor branch (Annex 5), who will in turn be responsible for notifying, the NI Audit Office and Department of Finance.

In the case where there is prima facie evidence that a fraud, or a bribery offence has been committed, the Director of Finance, in consultation with the Chief Executive, will consider if PSNI need to become involved.

The verbal report must be followed up, as soon as practicable with a written report addressed to the Director of Finance. The follow-up written report, should include all known facts relevant to the case. This may be treated as confidential and anonymous, if so, requested by the individual who raised the concerns.

It is important that Internal Audit is notified of possible fraud or bribery so that the effectiveness of existing internal controls can be reassessed, and additional control measures can be introduced if appropriate. The rapid discovery and proper reporting can also be an indicator of the strength of controls within a business area.

TNI will maintain a Fraud Log (Annex 6), containing details of actions taken in all cases. This log will be presented to the Audit and Risk Assurance Committee, who will bring any significant matters to the attention of the Board. All matters will be dealt with in confidence and in strict accordance with the terms of the Public Interest Disclosure (Northern Ireland) Order 1998 if appropriate.

3. Preliminary 'Fact-finding'

Before completing the written report described above, it may be necessary for line management to undertake an initial enquiry to ascertain the facts. This enquiry should be carried out as speedily as possible, after suspicion has been raised: prompt action is essential. The preliminary enquiry should consider the following aspects when a suspected fraud or bribery is reported:

- the source of discovery of the suspected irregularity;
- the authenticity of the information initially received; and
- the line management's initial assessment of the circumstances involved.

The purpose of the initial fact-finding exercise is to determine the factors that gave rise to the suspicion and to clarify whether a genuine mistake has been made or if it is likely that a fraud has been attempted or occurred, and a more detailed investigation needs to be instigated.

The Line Manager should not undertake preliminary enquiries until any suspicion has been reported to the Director of Finance, who will report to the Director of HR and Head of Internal Audit as appropriate. The Director of Finance, Internal Audit and the Director of HR will advise on an initial fact-finding exercise. This discreet preliminary enquiry should be carried out as speedily as possible. Where the suspected fraud involves the use of computers, advice must be sought from the TNI IT Manager before access or removal of computer equipment is attempted. Consideration should also be given to removing the suspect's access to computer systems.

It is imperative that such enquiries should not prejudice subsequent investigations or corrupt evidence, therefore, IF IN DOUBT, ASK FOR ADVICE.

If the preliminary enquiry confirms that a fraud has not been attempted or perpetrated, but indicates that internal controls are deficient, management should review their control systems with a view to ensuring that they are adequate and effective.

A robust review of the function/ directorate risk and control Framework should be conducted and where appropriate the Corporate Risk Register should also be reviewed. Internal Audit Service is available to offer advice and assistance on matters relating to internal control, if required.

4. Formal Reporting Stage

If the preliminary enquiry confirms the suspicion that a fraud has been attempted or perpetrated, management must ensure that all original documentation and computer-based files are preserved in a safe place for further investigation. Evidence must be carefully preserved; no marks should be made on original documents; and a record should be kept of anyone handling evidence. This is to prevent the loss or corruption of evidence, which may be essential to support subsequent disciplinary action or prosecution. The facts should be reported immediately to Director of Finance and Chief Executive to instigate a formal investigation.

To remove any threat of further fraud or loss, management should immediately change/strengthen procedures and if appropriate, consult the Head of HR regarding a precautionary suspension of any staff suspected of fraud or corruption.

Where the fraud has been perpetrated externally, management should consider suspending any payments or business with the company or individual and the need to inform other government departments or bodies.

5. Action Required for Internal Fraud

Where there is the suspicion of staff being involved (internal fraud) the Director of Finance, in consultation with the Director of HR and the Head of Internal Audit as appropriate , will decide on the appropriate course of action including internal reporting and oversight arrangements and the full formal investigation arrangements.

A TNI officer who is independent from the management of the business unit (who should be appointed by Director of Finance) should determine the scope of the investigation and set it out in a formal term of reference. The investigation will be led by Internal Audit Service and should be conducted by at least two officers, one of whom is trained in investigative techniques. An individual qualified in the use of the Police & Criminal Evidence (PACE) Act will be commissioned as appropriate. Should further expertise be required, e.g. Specialist Fraud Investigators, Solicitors, Forensic Accountants/Engineers, the Director of Finance will contact DfE sponsor who will advise us on the engagement of the appropriate assistance.

It is TNI's policy to suspend an individual suspected of fraudulent activity at the earliest juncture. Suspension itself does not imply guilt – it is simply another safeguard to prevent the removal or destruction or alteration of evidence.

6. Investigation of Suspected Fraud

The following best practice guidance must be applied (as appropriate) during any suspected fraud investigation:

- All aspects of the suspected officer's work should be investigated, not just the area where the fraud was discovered.
- The investigation will cover the period the officer was responsible for the processes under investigation, but consideration should also be given to investigating earlier periods of employment.
- Potential evidence, including paper files, computer files and records of amendments to files relevant to the case, should be retained securely (in compliance with PACE requirements) and not disposed of per normal routine procedures for disposal.
- Control weaknesses discovered in procedures during the investigation should be strengthened immediately to ensure that similar frauds or attempted frauds will not recur.
- The extent, if any, of supervisory failures should be examined.

7. Action Required for External Fraud

Where a fraud is suspected involving an external organisation or individual the Director / Head of Function should notify the Director of Finance and the Head of Internal Audit immediately. In these cases, it is the responsibility of Director of Finance, in consultation with the Head of Internal Audit and the relevant Director/ Head of Function, to determine an appropriate course of action. If there is sufficient evidence, the Head of Internal Audit, in consultation with the Head of Division, will notify the police. Thereafter, the investigation will be guided by police advice.

For a fraud occurring outside the jurisdiction of the UK, advice should be sought by the Director of Finance from the Head of Internal Audit or other appropriate persons as to the appropriate authorities to be notified.

8. Role of the Investigating Officer

The Investigating Officer should investigate all aspects of the suspected officer's work and not just the area where the fraud or bribe was discovered. The objective of the investigation is to:

- establish whether there is evidence that a fraud/ bribery has occurred;
- collect sufficient evidence to support any complaint to the police; and
- provide sufficient evidence for possible disciplinary or legal action.

The investigation should cover the period during which the Officer was responsible for the processes under investigation, but consideration should also be given to investigating earlier periods of employment. Potential evidence, including computer files and records of amendments relevant to the case, should be retained securely in compliance with PACE requirements.

Any control weaknesses discovered in procedures during the investigation should be strengthened immediately, and the extent of any supervisory failures examined.

It is the responsibility of the Investigating Officer to keep all other interested parties (Chief Executive, Director of Finance, Audit Committee, etc.) abreast of all developments.

When the Investigating Officer has completed his/her investigation, their report should be presented to the Chief Executive to be signed off.

The Director of Finance, in consultation with the Chief Executive, will consider Lessons learned which will be circulated to all other interested parties, who should take the appropriate action to improve controls to mitigate the scope for future recurrence of the fraud or bribery, and prevent any future

occurrences being committed. Where appropriate, the Chief Executive should discuss with the Head of Internal Audit the effect of any system weaknesses identified by the investigation.

9. Interviewing

Fraud investigation is a specialist area of expertise and staff tasked with carrying out an investigation should have appropriate experience and training. For the purposes of criminal proceedings, the admissibility of evidence is governed by the Police and Criminal Evidence (NI) Order 1989 (PACE). Documentary evidence must be properly recorded. It must be numbered and include an accurate description of when and where it was obtained as well as by and from whom. In criminal actions, evidence on or obtained from electronic media must have an accompanying document to confirm its accuracy.

In any investigation, there may be a need to interview staff, suspects or other persons involved. Interviewing is a specialist skill that is usually best carried out by or supported by the appropriate professionals.

When fraud or bribery is suspected, the need to interview can be for the purpose of disciplinary and/or criminal proceedings. When disciplinary action is necessary, interviews are usually carried out by the appropriate line manager in conjunction with a representative from Human Resources.

In these circumstances it is essential that specialist HR advice is sought on the appropriate disciplinary procedures before interviewing takes place. The potential involvement of the Police in any investigation does not negate the need to ensure that the appropriate disciplinary procedures have been followed.

When criminality is suspected, interviewing of suspects must not be carried out by staff, but must be left to the Police. If the conditions of the Police and Criminal Evidence (NI) Order 1989 (PACE) are not complied with, evidence will not be admissible in Court.

10. Liaison with the Police Service of Northern Ireland (PSNI)

A Memorandum of Understanding (MOU), setting out a basic framework for the working relationship between the PSNI and the public sector in respect of the investigation and prosecution of fraud or bribery cases, is in place. The MOU sets out a framework to ensure that appropriate action is taken by public sector organisations in line with DOF guidelines to deal with cases of suspected fraud, as set out in Managing Public Money Northern Ireland and other guidance issued by DOF. It also aims to ensure that actions throughout the investigative process are conducted in accordance with PACE where appropriate.

If the Chief Executive is satisfied that there is prima facie evidence of fraud, then in consultation with the DfE the matter will be reported to the PSNI in accordance with the operating protocols set out in the MOU.

Consultation with the Police at an early stage is beneficial, allowing the Police to examine the evidence available at that time and to make decisions on whether there is sufficient evidence to support a criminal prosecution or if a Police investigation is appropriate. Alternatively, the Police may recommend that TNI conducts further investigations and they will, more generally, provide useful advice and guidance on how the case should be taken forward.

If the Police decide to investigate, then it may be necessary for the Investigating Officer to postpone further internal action and adjust the investigation action plan as appropriate. However, the Investigating Officer should continue to liaise with the PSNI at regular intervals and report on progress made.

11. Post Event Action

Appropriate steps will be taken to recover all losses resulting from fraud, if necessary, through civil action. TNI solicitors should be consulted at an early stage on the recovery of assets, for example, action that might be taken to trace and freeze assets; action to prevent the release of assets; obtaining search orders.

Where a fraud, or attempted fraud, has occurred, management must make any necessary changes to systems and procedures to ensure that similar frauds or attempted frauds will not recur. Additionally, if a TNI employee is suspected of involvement, the Director of Finance in conjunction with the Director of HR will consider the appropriate course of action. This may range from close monitoring/supervision to re-location, or precautionary suspension. It should be noted, however, that suspension does not in any way imply guilt.

Internal Audit Service is available to offer advice and assistance on matters relating to internal control, if considered appropriate.

In the event of media enquiries during the course of an investigation, TNI's Communication Officer should consult with the Director of Finance, the Head of Internal Audit and the Director of HR to determine what information can be released.

The Director of Finance and TNI's FOI Officer should be consulted in the event of a Freedom of Information Request relating to an investigation being received.

Following an investigation, a report will be compiled by the Investigating Officer outlining all aspects of the fraud or attempted fraud: that is, the cause, how it was detected, the investigation process, control weaknesses, and how similar frauds or attempted frauds can be prevented in future. The report will be provided, in the first instance, to the Director of Finance and the Chief Executive. If appropriate the report, or extracts of the report, will be circulated throughout TNI. Consideration will also be given to informing other public sector organisations. At an appropriate time, the NICS Fraud Forum will also be informed of the lessons learned.

12. Reporting Arrangements

TNI's Audit & Risk Assurance Committee shall be kept informed of progress during and at the conclusion of an investigation.

TNI's Finance team will submit annual fraud returns to DFE and DFE's Accountability and Casework Branch will be responsible for compiling the annual return of frauds to DFP (Fraud and Internal Audit Policy), in accordance with Annex 4.7 of MPMNI requirements.

Annexes

Annex 1: Sources of Further Information

Further information and guidance to supplement this document is available from the following sources:

Managing Public Money Northern Ireland (MPMNI)

This document sets out the main principles for dealing with resources used by public sector organisations in Northern Ireland. It can be accessed via the following link:

http://www.afmdni.gov.uk/frab/browse.asp?branch=1&category=43&maxres=20&start=0&orderby=3

Standards in Public Life - The Seven Principles

The Nolan Committee was established by central government to review standards of behaviour in all areas of the public sector. Its report defined the seven guiding principles that apply to public servants. Our policies and procedures reflect these seven principles as detailed in Annex A.

Memorandum of Understanding (MOU) with PSNI

A Memorandum of Understanding (MOU) is in place with the PSNI setting out the working relationship between the Northern Ireland public sector and PSNI in respect of the investigation and prosecution of suspected fraud cases. The MOU sets out best practice and business areas should ensure that the guidance is adhered to. The MOU can be viewed via the following link:

www.afmdni.gov.uk/fiap/browse.asp?branch=3&category=15&maxres=20&start=0&orderby=2

Managing the Risk of Fraud – A Guide for Managers

This document is available via the link below:

http://www.afmdni.gov.uk/fiap/browse.asp?branch=3&category=15&maxres=20&start=0&orderby=2

Guidance on the Provision of Gifts and Hospitality

There are strict rules governing expenditure by NIPF staff on hospitality and official gifts and on the acceptance of gifts, hospitality or awards. It is essential that staff adhere to the principles, guidelines and procedures set out the NIPF gifts and hospitality policies. Anyone involved in anti-fraud procedures is encouraged to read these documents.

Annex 2: Fraud Indicators

Fraud indicators are clues or hints that a closer look should be made at an individual, area or activity.

Examples of issues that could be investigated to ensure fraud is not taking place include:

1. Unusual employee behaviour (e.g. a supervisor who opens all incoming mail, refusal to comply with normal rules and practices, failure to take leave, managers by-passing subordinates, subordinates by-passing managers, living beyond means, regular long-hours working, job dissatisfaction/unhappy employee, secretiveness or defensiveness).
2. Unrecorded transactions or missing records (e.g. invoices or contracts).
3. Disorganised operations in such areas as accounting, purchasing or payroll.
4. Crisis management coupled with a pressured business environment.
5. Absence of controls and audit trails (e.g. Inadequate or no segregation of duties, lack of rotation of duties).
6. Low levels of review or approval.
7. Policies not being followed.
8. Inadequate monitoring to ensure that controls work as intended (periodic testing and evaluation).
9. Lack of interest in, or compliance with, internal controls.
10. Documentation that is photocopied or lacking essential information.
11. Alterations to documents.
12. Missing documents such as expenditure vouchers and official records.
13. Excessive variations to budgets or contracts.
14. Bank and ledger reconciliations are not maintained or cannot be balanced.
15. Excessive movements of cash or transactions between accounts.
16. Numerous adjustments or exceptions.
17. Duplicate payments.
18. Large payments to individuals.
19. Unexplained differences between inventory checks and asset or stock records.
20. Transactions not consistent with the entity's business
21. Deficient screening for new employees including casual staff, contractors and consultants.
22. Employees in close relationships in areas where segregation of duties is a key control.
23. Unauthorised changes to systems or work practices.
24. Lowest tenders or quotes passed over with minimal explanation recorded.
25. Single vendors.
26. Unclosed but obsolete contracts.
27. Defining needs in ways that can be met only by specific contractors.
28. Splitting up requirements to get under small purchase requirements or to avoid prescribed controls.
29. Suppliers/contractors who insist on dealing with one particular member of staff.
30. Vague specifications.
31. Disqualification of any qualified bidder.
32. Chronic understaffing in key control areas.
33. Excessive hours worked by key staff.
34. Consistent failures to correct major weaknesses in internal control.
35. Management frequently overrides internal control.
36. Lack of common sense controls such as changing passwords frequently, requiring two signatures on cheques or restricting access to sensitive areas.

Annex 3: Common Methods and Types of Fraud

1. Payment for work not performed
2. Forged endorsements
3. Altering amounts and details on documents
4. Collusive bidding
5. Overcharging
6. Writing off recoverable assets or debts
7. Unauthorised transactions
8. Selling information
9. Altering stock records
10. Altering sales records
11. Cheques made out to false persons
12. False persons on payroll
13. Theft of official purchasing authorities such as order books
14. Unrecorded transactions
15. Transactions (expenditure/receipts/deposits) recorded for incorrect sums
16. Cash stolen
17. Supplies not recorded at all
18. False official identification used
19. Damaging/destroying documentation
20. Using copies of records and receipts
21. Using imaging and desktop publishing technology to produce apparent original invoices
22. Transferring amounts between accounts frequently
23. Delayed terminations from payroll
24. Bribes
25. Over-claiming expenses
26. Skimming odd pence and rounding
27. Running a private business with official assets
28. Using facsimile signatures
29. False compensation and insurance claims
30. Stealing of discounts
31. Selling waste and scrap.

Annex 4: Examples of Good Management Practices - Reducing Opportunities for Fraud.

Introduction

The absence of proper control and the failure to observe existing control procedures are the main contributory factors in most frauds.

Managers must ensure that the opportunities for fraud are minimised. Separation of duties, effective procedures and checks should prevent or deter fraud from occurring. 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;
- Through the "fear factor" (i.e. the risk of being caught or the severity of the consequences);
- By changing attitudes to fraud; and
- By making it too much effort to commit.

Below are only some examples of the types of control that can be used to prevent or detect fraud. For examples of internal controls in specific areas see the DFP publication "Managing the Risk of Fraud – A Guide for Managers".

Internal Control

A 'Control' is any action, procedure or operation undertaken by management to increase the likelihood that activities and procedures achieve their objectives. Control is a response to risk – it is intended to contain uncertainty of outcome.

Some frauds arise because of a system weakness such as a lack of proper control over e.g. placing of purchase orders. Other frauds are the result of failures to follow proper control procedures. It may be the result of carelessness in carrying out a check, or it may be that too much trust has been placed in one individual with no effective separation of duties. Frauds that result from collusion may be more difficult to detect and prevent as these types of fraud tend to operate within the normal control environment.

In designing control, it is important that the control put in place is proportional to the risk. In most cases it is normally sufficient to design control to give a reasonable assurance of confining loss within the risk appetite of the organisation. Every control action has an associated cost, and it is important that the control action offers value for money in relation to the risk that it is controlling. Generally speaking, the purpose of control is to contain risk to a reasonable level rather than to remove it entirely.

When risks and deficiencies in the level of control are identified it is necessary to choose the most appropriate type of controls within the above guidelines. In respect of fraud risks prevention is almost always preferable to detection. Strong preventive controls should therefore be applied wherever possible.

The following range of controls should be considered always ensuring that a balance between identified risk and value for money is maintained:

Physical security

This is a preventive measure which controls or monitors access to assets, documentation or IT systems to ensure that there is no unauthorised use, loss or damage.

Assets can range from the computer terminal that sits on the desk to the cheques sent out to pay suppliers. As a general principle all assets should be held securely and access to them restricted as appropriate. The control should apply not only to the premises but also to computers, databases, banking facilities, documents and any

other area that is critical to the operation of the individual organisation. It may even be appropriate to restrict knowledge of the existence of some assets.

Access to computer systems is an important area that should be very tightly controlled, not only to prevent unauthorised access and use, but also to protect the integrity of the data - the Data Protection Act requires computer and data owners to secure information held on their systems which concerns third parties. The threat to computers can come from both inside and outside an organisation. This threat may increase with the introduction of systems to meet the e-Government target (e.g. to allow the public to do business electronically with government departments, to link public sector computer systems etc). Computers are also vulnerable to theft, both in terms of hardware and software. This type of theft has the additional cost of potential major disruption to the core operations of an organisation.

Organising

organising involves the allocation of responsibility to individuals or groups so that they work together to achieve objectives in the most efficient manner. Major principles in organising relevant to fraud are:

- Clear definition of the responsibilities of individuals for resources, activities, objectives and targets. This includes defining levels of authority. This is a preventive measure which sets a limit on the amounts which may be authorised by individual officers. To be effective, checks need to be made to ensure that transactions have been properly authorised;
- Establishing clear reporting lines and the most effective spans of command to allow adequate supervision;
- Separating duties to avoid conflicts of interest or opportunities for abuse. This is also largely a preventive measure which ensures that the key functions and controls over a process are not all carried out by the same member of staff (e.g. ordering goods should be kept separate from receipt of goods); similarly, authorisation and payment of invoices; and
- Avoiding undue reliance on any one individual.

Supervision and checking of outputs

Supervision is the function by which managers scrutinise the work and performance of their staff. It provides a check that staff are performing to meet standards and in accordance with instructions. It includes checks over the operation of controls by staff at lower levels. These act as both preventive and detective measures and involve monitoring the working methods and outputs of staff. These controls are vital where staff are dealing with cash or accounting records. Random spot checks by managers can be an effective anti-fraud measure.

Audit trail

This is largely a detective control, although its presence may have a deterrent effect and thus prevent a fraud. An audit trail enables all transactions to be traced through a system from start to finish. In addition to allowing detection of fraud it enables the controls to be reviewed.

Monitoring

Management information should include measures and indicators of performance in respect of efficiency, effectiveness, economy and quality of service. Effective monitoring, including random checks, should deter and detect some types of fraudulent activity.

Evaluation

Policies and activities should be evaluated periodically for economy, efficiency and effectiveness. The management of the operation may perform evaluations, but they are usually more effective when performed by an independent team. Such evaluations may reveal fraud.

Staffing

Adequate staffing is essential for a system to function effectively. Weaknesses in staffing can negate the effect of other controls. Posts involving control of particularly high value assets or resources may need the application of additional vetting procedures. Rotation of staff between posts can help prevent or detect collusion or fraud.

Asset Accounting

Asset registers used for management accounting purposes can help detect losses that may be caused by fraud.

Budgetary and other financial controls

Use of budgets and delegated limits for some categories of expenditure and other accounting controls should ensure that expenditure is properly approved and accounted for by the responsible manager. This should limit the scope for fraud and may result in some types of fraud being detected.

Systems development

Controls over the development of new systems and modifications to existing systems or procedures are essential to ensure that the effect of change is properly assessed at an early stage and before implementation. Fraud risks should be identified as part of this process and the necessary improvements in control introduced.

Annex 5 : Pro Forma - Initial Fraud Notification to DfE

DoF Pro-forma: Initial Fraud Notification to Department

The information below is required if known at the date of reporting. If bodies wish to use a different format for notifications, it should provide the same relevant details.

1.	Departmental fraud reference number (unique identifier)	
2.	Department	
3.	Name of body (e.g. specific Board, Trust, NDPB, Agency etc)	
4.	Specific location of fraud (e.g. name of school, name of depot etc)	
5.	Date fraud or suspected fraud discovered	
6.	Is the case being reported as actual, suspected or attempted fraud?	
7.	Type of fraud?	
8.	What was the cause of the fraud?	
9.	Brief outline of case	
10.	Amount of lost or estimated value?	
11.	How was the fraud discovered?	
12.	Who perpetrated the fraud?	
13.	Has PSNI been notified?	
14.	Any other action taken so far?	
15.	Please give contact details for this fraud in case follow-up is required	

Annex 6 Fraud Log

Tourism NI

Log of reported Irregularities under the Anti-Fraud and Anti-Bribery Response Plan

Case No	Detais of suspected irregularity	Notified by / how identified	Date	Estimated loss £	Case Manager	Action plan	Current status