Department of Finance
An Roinn Airgeadais
www.finance-ni.gov.uk

DEPARTMENT OF FINANCE

ANTI-FRAUD POLICY

DOCUMENT CONTROL

(i) SUMMARY

This document provides guidance for Department of Finance (DoF) staff and non-staff in respect of the Fraud Response Plan.

(ii) DOCUMENT STATUS HISTORY

Version	Issue Date	Section	Reason for Update
1.0	December 2021	Key Contacts	Key contacts updated
1.1	September 2023	Whole Document	Key contacts updated, document control added, refresh of terminology used and links updated.
1.2	April 2024	Key Contacts	Key contacts updated

(ii) DOCUMENT REVIEW DATE

This document will be reviewed on or before;

April 2025

Contents

INTRODUCTION BY DEPARTMENTAL ACCOUNTING OFFICER

There is a continuing need to raise staff awareness of our responsibility to safeguard public resources against the risk of fraud. This paper sets out our Department's **Anti- Fraud Policy.** There is a separate **Fraud Response Plan** that details those actions which must be taken by Business Areas in the event of a fraud, attempted fraud or irregular activity being suspected.

Fraud is not a victimless crime. We are entrusted with taxpayers' money, and we must look after it in the same way that we look after our own. So we must all be aware of:

- what constitutes fraud;
- the potential for fraud;
- steps to prevent fraud in the first instance; and
- what to do in the event of fraud or if we suspect fraud has occurred.

The Department takes a **zero tolerance approach** to fraud, reporting instances of fraud to the police as necessary, and taking all appropriate steps to recover monies lost as a result of fraud perpetrated against the Department.

All cases of suspected or actual fraud should be reported immediately to the Finance Director who will advise management on what steps to take next.

If staff become aware of wrongdoing there may be some circumstances where they are afraid to voice their concern, especially if the case involves a more senior officer. The Public Interest Disclosure (Northern Ireland) Order 1998 protects individuals from workplace retributions for raising a genuine concern whether a risk to the public purse or other wrongdoing. The Department has a **Raising Concerns (Whistleblowing Policy)** to assure you that it is safe to speak up if you are concerned about something.

Please ensure that you familiarise yourself with your anti-fraud responsibilities and the steps which you must take in the event of fraud or suspected fraud (see the Fraud Response Plan).

IF IN DOUBT, ASK FOR ADVICE

NEIL GIBSON

1 INTRODUCTION

1.1 The Department's **Anti-Fraud Policy** sets out the actions we must take and the responsibilities we have to help prevent fraud. This document relates to fraud and loss within the Department, its Agency and Arms Length Bodies, and applies to **all monies for which the Department is accountable, including**: departmental income and expenditure; Special EU Programmes Body; the Principal Civil Service Pension Scheme (NI); and rates collection.

1.2 The Department 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 must be a concern to all members of staff. The Department takes a **zero tolerance** approach and will not therefore tolerate any level of fraud or corruption; consequently, departmental policy is to thoroughly investigate all suspected frauds and allegations (anonymous or otherwise) and where appropriate, refer to the police at the earliest juncture and seek recovery of all losses, if necessary through civil action. The Department is also committed to ensuring that opportunities for fraud and corruption are reduced to the lowest possible level of risk.

2 DEFINITION OF FRAUD

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

2.2 Fraud is not a victimless crime and is generally used to describe such acts as deception, bribery, money laundering, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion.

2.3 Computer fraud is where information technology (IT) equipment has been used to manipulate computer programs or data dishonestly (for example by altering or substituting records, destroying or suppressing records, duplicating or creating spurious records), or where the existence of an IT system was a material factor in the perpetration of fraud (i.e. where the fraud was unlikely to have occurred if there had been no IT system). Theft or fraudulent use of computer facilities, computer programs and the Internet is included in this definition. The suspicion that any of these acts have taken place should be regarded as potentially fraudulent.

2.4 The Fraud Act 2006 came into effect on 15th January 2007. The Act states that a person is guilty of fraud if someone is in breach of any of the following:

- **Fraud by false representation**, i.e. if someone 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;
- **Fraud by failing to disclose information**, i.e. if someone dishonestly fails to disclose to another person information which he is under a legal duty to disclose and intends, by means of abuse of that position, to make a gain for himself or another, or to cause loss to another or expose another to risk of loss; and
- **Fraud by abuse of position**, i.e. if someone 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.

2.5 At a basic level four elements are normally necessary for a fraud to occur:

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

2.6 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. While some people would never contemplate perpetrating a fraud, others may if they thought they could do it without being detected. A high chance of being caught will often deter such individuals.

3 DEPARTMENT'S RESPONSIBILITIES

3.1 The Department's responsibilities are set out in this document. Further detail can be found in Annex 4.7 of "Managing Public Money Northern Ireland" (MPMNI) and in guidance contained on the Accountability and Financial Management Division (AFMD) website: Accountability and Financial Management DoF. AFMD also publishes the NICS Annual Fraud Report.

3.2 The Department's Accounting Officer is responsible for establishing and maintaining a sound system of internal control that supports the achievement of departmental policies, aims and objectives. The system of internal control is designed to respond to and manage the whole range of risks that a department faces. The system of internal control is based on an on-going process designed to identify the principal risks, to evaluate the nature and extent of those risks and to manage them effectively. Managing fraud risk will be seen in the context of the management of this wider range of risks.

3.3 Overall responsibility for managing the risk of fraud has been delegated to the **Finance Director**. Other departmental directors also have a key responsibility to take steps, as are reasonably open to them, to prevent and detect fraud.

3.4 Responsibilities of the **Finance Director** include:

(a) Developing the Department's Fraud Risk Register and overseeing regular reviews of the Corporate fraud risks assessments in order to keep the Register current (see section 11);

(b) Establishing an effective anti-fraud policy and fraud response plan, commensurate to the level of fraud risk identified in the Department's Fraud Risk Register;

(c) Designing an effective control environment to prevent fraud commensurate with the level of fraud risk;

(d) Assessing the risk of the Department being used for money laundering;

(e) Advising departmental directors on the conduct of fraud investigations, and liaising where necessary with Group Fraud Investigation Services (GFIS), and the Head of Internal Audit in accordance with the Fraud Response Plan;

(f) Ensuring that vigorous and prompt investigations are carried out if fraud occurs, is attempted or is suspected and appropriate action is taken to recover assets and losses;

(g) Establishing appropriate mechanisms for:

- Reporting fraud risk issues;
- Reporting significant incidents of fraud to the Accounting Officer;
- Staff to report all instances of suspected or actual fraud to line management/Head of Branch who must then report to the Finance Director;
- Reporting, externally, to AFMD and the Comptroller and Auditor General, Northern Ireland Audit Office (NIAO), in accordance with MPMNI Annex 4.7;
- Coordinating assurances about the effectiveness of the anti-fraud policy and fraud response plan to support the Department's annual Governance Statement;
- Liaising with the Departmental Audit and Risk Committee;
- Making sure that all staff are aware of the organisation's anti-fraud policy and know what their responsibilities are in relation to combating fraud; and
- Ensuring that appropriate action is taken to minimise the risk of similar frauds occurring in future.

3.5 The **NICS HR Director** also has specific responsibilities which include ensuring that:

(a) Appropriate pre-employment screening measures are undertaken;

(b) Anti-fraud awareness training is provided as appropriate and, if necessary, more specific anti-fraud training and development is provided to relevant staff;

(c) Providing advice and support to management in implementing suspensions and any subsequent disciplinary investigation, including advising on the application of the NICS Disciplinary Policy;

(d) Where appropriate, legal and/or disciplinary action is taken against perpetrators of fraud;

(e) Where appropriate, disciplinary action is taken against supervisors where supervisory failures have contributed to the commission of fraud; and

(f) Where appropriate, disciplinary action is taken against staff who fail to report fraud.

3.6 Responsibilities of all **Departmental Directors** include:

(a) Taking steps to provide reasonable assurance that the activities of the Department are conducted honestly and that its assets are safeguarded, including assessing the fraud risk involved in the operations/area for which they are responsible;

(b) Signing off the business area's fraud risk assessment(s) every 6 months and on each occasion they are amended (if sooner);

(c) Ensuring, that to the best of their knowledge and belief, financial information, whether used in the Department's operations, business or for financial reporting, is reliable;

(d) Establishing arrangements designed to deter fraudulent or other dishonest conducts and ensuring that these arrangements are complied with;

(e) Where a fraud has taken place, implementing new controls to reduce the risk of similar fraud;

(f) Reporting any instances of suspected or proven fraud to the Finance Director as soon as they become aware of such instances;

(g) Where appropriate overseeing the conduct of fraud investigations and liaising where necessary with the Finance Director in accordance with the Fraud Response Plan;

(h) Ensuring that appropriate action is taken to recover assets and losses; and

(i) Providing updates on open fraud cases.

4 LINE MANAGER'S RESPONSIBILITIES

4.1 Line managers are responsible for ensuring that an adequate system of internal control exists within their areas of responsibility and that controls operate effectively. **Responsibility for the prevention and detection of fraud, therefore, rests primarily with managers.**

4.2 A major element of good corporate governance is a sound assessment of the organisation's business risks. Managers need to ensure that:

(a) Fraud risks have been identified within risk registers based on a review of the operations/area for which they are responsible;

(b) Each risk has been assessed for likelihood and potential impact;

(c) Adequate and effective controls have been identified for each risk;

(d) Controls are being complied with, through regular review and testing of control systems;

(e) Risks are reassessed as result of the introduction of new systems or amendments to existing systems;

(f) Where a fraud has occurred, or has been attempted, controls are reviewed and new controls implemented, as necessary, to reduce the risk of fraud recurring; and

(g) Fraud occurrences are quantified on an annual basis and Risk Registers updated 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.

4.3 In terms of establishing and maintaining effective controls, it is generally desirable that:

(a) There is a regular rotation of staff, particularly in key posts;

(b) Wherever possible, there is a separation of duties so that control of a key function is not vested in one individual;

(c) Backlogs are not allowed to accumulate; and

(d) In designing any new system, consideration is given to building in safeguards to prevent and/or detect internal and external fraud.

4.4 As fraud prevention is the ultimate aim, anti-fraud measures should be considered and incorporated in every system and programme at the design stage, e.g. the design of application forms, regular monitoring of expenditure etc. Internal Audit is available to offer advice to managers on risk and control issues in respect of existing and developing systems/programmes.

5 STAFF RESPONSIBILITES

5.1 Every member of staff has a duty to ensure that public funds are safeguarded and therefore, **everyone is responsible** for:

- Acting with propriety in the use of official resources and the handling and use of public funds in all instances. This includes cash and/or payment systems, receipts and dealing with suppliers;
- Conducting themselves in accordance with the seven principles of public life detailed in the first report of the Nolan Committee 'Standards in Public Life',

  i.e. selflessness, integrity, objectivity, accountability, openness, honesty and leadership; and
- Being vigilant 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. **Appendix 1** provides examples of Indicators of Fraud. In addition, Risks and Controls in Specific Systems are included in **Appendix 2**, with guidance on Reducing Opportunities for Fraud detailed in **Appendix 3**.

5.2 In addition, it is the **responsibility** of every member of staff to report details immediately to their line manager/Head of Branch or the Finance Director if they suspect that a fraud has been attempted or committed, or see any suspicious acts or events. More details on reporting are included in the Department's **Fraud Response Plan**. The Public Interest Disclosure (NI) Order 1998 – see CSC 04/03 Guidance on Public Interest Disclosure (Raising Concerns - 'whistleblowing') – protects the rights of staff who report wrongdoing. If you are in any doubt, you should speak to a senior officer. A **DoF Raising Concerns (Whistleblowing) Policy** has been developed and can be found on the DoF Internet, and information is also available in **Appendix 4**.

5.3 A description of the constitutional position of civil servants and the values they are expected to uphold is given in the **NICS Code of Ethics**. (See NICS Staff Handbook – HRConnect Portal), and details of the Department's **CLEAR (Customer, Leadership, Ethical, Accountable, Results)** values can be found on the Department's website.

5.4 Advice is also available through the independent charity Protect (previously known as Public Concern at Work) on **020 3117 2520**. Their lawyers can give free confidential advice at any stage regarding a concern about serious malpractice at work. An employee can, of course, also seek advice from a lawyer of their own choice, at their own expense.

5.5 Section 5 of the Criminal Law Act (Northern Ireland) 1967 (Withholding Information) also places the onus on individuals to report/pass evidence to the Police. The involvement of the Police Service of Northern Ireland (PSNI) is dealt with in the **Fraud Response Plan**.

5.6 Staff must also assist any investigations by making available all relevant information, by co-operating in interviews and if appropriate provide a witness statement.

5.7 As stewards of public funds, civil servants must have, and be seen to have, high standards of personal integrity. Staff including temporary staff or contractors should not accept gifts, hospitality or benefits from a third party, which might be seen to compromise their integrity. The Department has specific guidance on **The Provision and Acceptance of Gifts and Hospitality**, and this guidance also applies to gifts or hospitality offered to spouses, partners or other associates of an official if it could be perceived that the gift or hospitality is in fact for the benefit of the official. The guidance, setting out the fundamental principles for the provision and acceptance of gifts, hospitality and rewards, can be found on the Department's Intranet.

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

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 Department 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. Risk and Control Frameworks are also reviewed as a constituent part of each audit assignment to ensure that management have reviewed their risk exposures and, where appropriate, identified the possibility of fraud as a business 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. However, discussion of a case with internal audit does not remove the need for staff to ensure that all cases of suspected or actual fraud are reported immediately to the Finance Director.

7 FRAUD INVESTIGATION

7.1 Line managers should be alert to the possibility that unusual events or transactions can be symptoms of fraud or attempted fraud. Fraud may also be highlighted as a result of specific management checks or be brought to management's attention by a third party. It is departmental policy that there will be consistent handling of all suspected fraud cases without regard to position held or length of service, and investigators should have free access to all staff, records and premises in order to carry out investigations.

7.2 After suspicion has been roused, prompt action is essential, and all cases of suspected or actual fraud should be reported immediately to the Finance Director who can provide advice on next steps.

7.3 Line management **should not** undertake preliminary enquiries until any suspicion has been reported to and advice taken from the Finance Director. **As detailed in the Fraud Response Plan, it is imperative that enquiries should not prejudice subsequent investigations or corrupt evidence, therefore,**

7.4 If an initial examination confirms the suspicion that a fraud has been perpetrated or attempted, management should follow the procedures provided in the Department's **Fraud Response Plan**.

8 GROUP FRAUD INVESTIGATION SERVICE (GFIS)

8.1 The Department uses the Group Fraud Investigation Service (GFIS) to conduct fraud investigations. This unit is led by the Group Head of Internal Audit and Fraud Investigation Services, Tracey McCavigan and is based at Hillview Buildings, Stormont Estate, Belfast. The contact number is 028 91 279669 or ext 59669.

8.2 The Group Service provides fraud investigation services to the Department, its agency and Arm's Length Bodies in line with a Service Level Agreement agreed between the Group Service and the Department.

8.3 The Group Service can be contacted directly to obtain advice and assistance on fraud related matters, however, business areas wishing to refer cases for investigation should contact the Departmental Finance Director in the first instance.

9 DoF FRAUD WORKING GROUP

9.1 The DoF Fraud Working Group provides a strategic overview of counter fraud activities within the Department, its Agency and Arms Length Bodies. In particular the Group has the following ambit:

- Monitor and review, and disseminate as necessary, outputs of the NICS Fraud Forum;
- Coordinate the work being done in the Department on tackling fraud and provide a forum for the exchange of information/sharing of experience for mutual benefit;
- Periodically review the DoF Anti-Fraud Policy and Fraud Response Plan for relevance and currency;
- Identify departmental training needs and assist in the coordination of training to meet needs;

- Share best practice and examples of anti-fraud measures and procedures; and
- Monitor trends/occurrences of fraud both within and outside the Department and disseminate, as necessary, lessons learned.

9.2 The Group is chaired by the Department's Finance Director and is attended by the Head of Internal Audit. The membership of the Group includes a representative from each of DoF's Directorates and Agencies. The DoF representative on the NICS Fraud Forum will also have membership to facilitate dissemination of information from the Fraud Forum and provide a conduit for feedback. Membership is flexible and may include other interested parties as the occasion demands.

9.3 The Fraud Working Group meets or corresponds as required and at least annually. The Departmental Audit and Risk Committee are advised of discussions and activities undertaken by the group.

10 NATIONAL FRAUD INITIATIVE

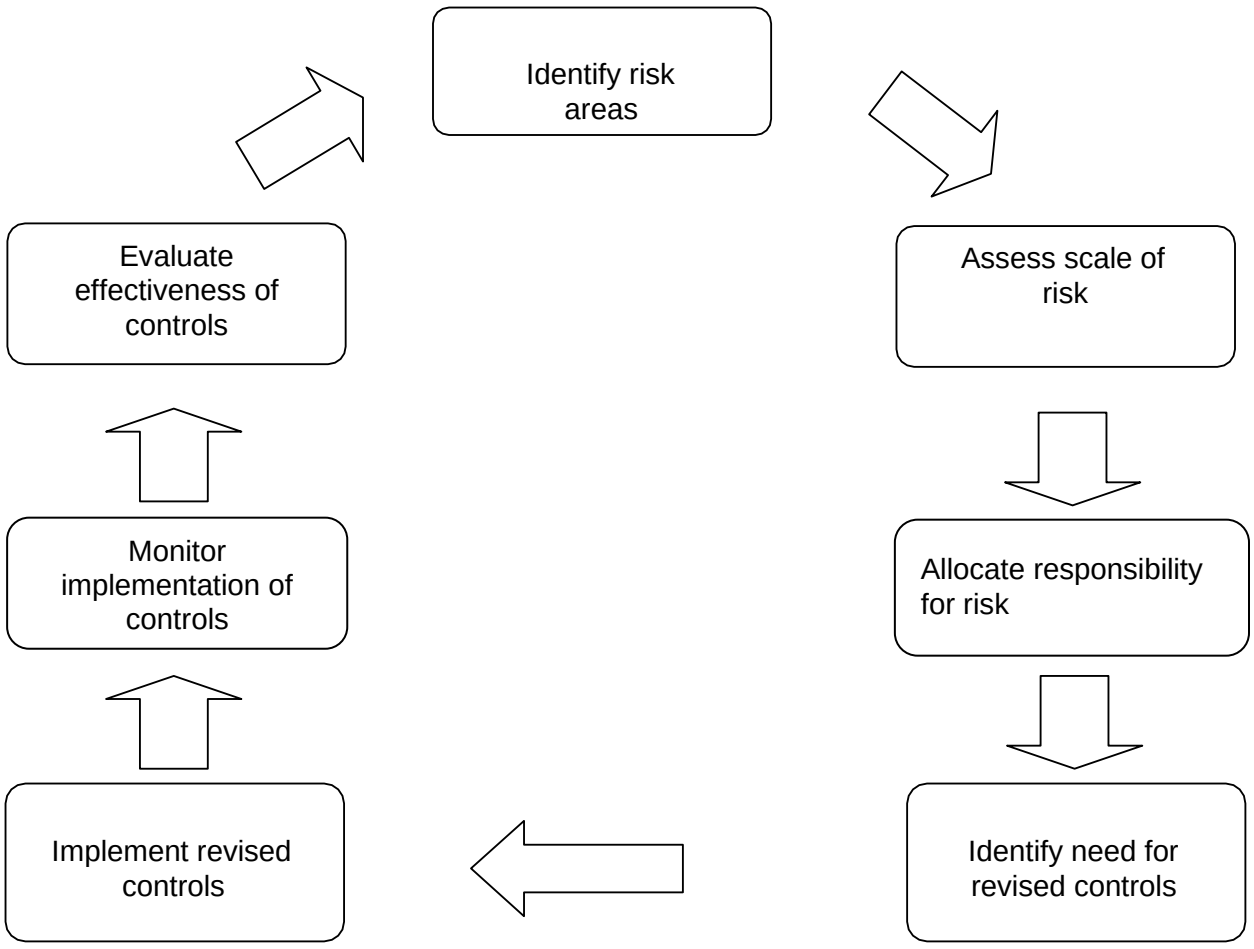
10.1 The National Fraud Initiative (NFI) is an effective data matching exercise. It compares information held by different organisations and within different parts of an organisation to identify potentially fraudulent claims and overpayments. The Comptroller and Auditor General for Northern Ireland can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

10.2 The Department provides payroll, pensions, trade creditors, rate relief and domestic rates data sets to identify cases of suspected fraud and overpayments. Participation in the NFI represents a key strand of the Department's anti-fraud policy.

11 FRAUD RISK ASSESSMENTS

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

Figure 1: RISK ASSESSMENT CYCLE



12 DISCIPLINARY ACTION

12.1 After full investigation the Department will take legal and/or disciplinary action in all cases where it is considered appropriate. Any member of staff found guilty of a criminal act will be considered to have committed a serious disciplinary offence and will be dismissed from the Department on the grounds of gross misconduct.

12.2 Where supervisory negligence is found to be a contributory factor, disciplinary action may also be initiated against those managers/supervisors responsible.

12.3 It is departmental policy that, where appropriate, all cases of fraud, whether perpetrated or attempted by a member of staff or by external organisations or persons, will be referred to the PSNI at the earliest possible juncture.

12.4 Appropriate steps will be taken to recover all losses resulting from fraud, if necessary through civil action.

13 MALICIOUS ALLEGATIONS

13.1 If an allegation is made frivolously, in bad faith, maliciously or for personal gain, disciplinary action may be taken against the person making the allegation.

14 CONCLUSION

14.1 It is appreciated that the circumstances of individual frauds will vary. The Department takes fraud very seriously, taking a **zero tolerance** approach, and will ensure that all cases of actual or suspected fraud, including attempted fraud, are vigorously and promptly investigated and that appropriate remedial action is taken, including recovery of losses. Managers should be fully aware of their responsibility to protect public funds and as such, should always be alert to the potential for fraud.

14.2 Any queries in connection with this **Anti-Fraud Policy** should be directed to the Finance Director.

14.3 Current contact details are provided in **Appendix 7.**

DEPARTMENT OF FINANCE

ANTI-FRAUD POLICY APPENDICIES

Appendix 1 - INDICATORS OF FRAUD

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:

- Unusual employee behaviour (e.g. a supervisor who opens all incoming mail, refusal to comply with normal rules and practices, fails to take leave, managers by-passing subordinates, subordinates by-passing managers, living beyond means, regular working of long hours, job dissatisfaction/unhappy employee, secretiveness or defensiveness).
- Unrecorded transactions or missing records (e.g. invoices, contracts).
- Disorganised operations in such areas as accounting, purchasing or payroll.
- Crisis management coupled with a pressured business environment.
- Absence of controls and audit trails (e.g. inadequate or no segregation of duties, lack of rotation of duties).
- Low levels of review or approval.
- Policies not being followed.
- Inadequate monitoring to ensure that controls work as intended (periodic testing and evaluation).
- Lack of interest in, or compliance with, internal controls.
- Documentation that is photocopied or lacking essential information.
- Alterations to documents.
- Missing documents such as expenditure vouchers and official records.
- Excessive variations to budgets or contracts.
- Bank and ledger reconciliations are not maintained or cannot be balanced.
- Excessive movements of cash or transactions between accounts.
- Numerous adjustments or exceptions.
- Duplicate payments.
- Large payments to individuals.
- Unexplained differences between inventory checks and asset or stock records.
- Transactions not consistent with the entity's business.
- Deficient screening for new employees including casual staff, contractors and

consultants.

- Employees in close relationships in areas where segregation of duties is a key control.
- Unauthorised changes to systems or work practices.
- Lowest tenders or quotes passed over with minimal explanation recorded.
- Single vendors.
- Unclosed but obsolete contracts.
- Defining needs in ways that can be met only by specific contractors.
- Splitting up requirements to get under small purchase requirements or to avoid prescribed controls.
- Suppliers/contractors who insist on dealing with one particular member of staff.
- Vague specifications.
- Disqualification of any qualified bidder.
- Chronic understaffing in key control areas.
- Excessive hours worked by key staff.
- Consistent failures to correct major weaknesses in internal control.
- Management frequently override internal control.
- Lack of common sense controls such as changing passwords frequently, requiring two signatures on cheques or restricting access to sensitive areas.

Appendix 2 - EXAMPLES OF RISKS AND CONTROLS IN SPECIFIC SYSTEMS

Cash Handling

There are many risks associated with cash handling. Theft or misappropriation of cash may be assisted by the suppression, falsification or destruction of accounting records, or where no initial records are created at all. This section suggests some controls that should be in place.

How fraud could be perpetrated	**Examples of controls**
Theft	• Hold cash securely at all times. • Restrict access to cash to named personnel. • Hold keys securely and limit access to authorised personnel. Keep cash balances to a minimum. • Maintain transaction records. • Carry out periodic and independent checks and reconciliations.
Income received not brought to account	• Issue pre-numbered receipts (ideally receipts should be generated automatically). Maintain prompt and accurate records of income received. • Ensure post-opening duties are carried out by at least two people and receipts log completed and signed by both officers. • Separate duties at key stages of the process: - bringing receipts to account and preparation of cash and cheques for banking - daily cash balancing and bank reconciliations. • Establish regular and random management checks of source documentation, accounting records and bank reconciliations. • Rotate staff duties frequently.
Illegal transfer or diversion of money. Changes and additions to payee details through BACS.	• Ensure that changes and additions to payee details and other standing data are properly authorised. • Restrict and log system access to make and authorise these changes. • Provide adequate supervision of all staff particularly new, inexperienced or temporary staff. • Ensure payments are authorised before they are made. • Restrict knowledge of transfer codes (and passwords if payments are initiated internally by computer) to approved personnel. • Change transfer codes and passwords frequently and always when staff leave. Passwords and User Ids should always be suspended when a member of staff leaves. Ensure that payment reports are independently reviewed for accuracy immediately before the transfer of funds occurs. • Separate duties (e.g. between those setting up payment accounts and those authorised • to trigger payments and between those receiving goods and services and those who process and make payments).

Accounting records are falsified or amended to allow unauthorised payments	• Ensure that amendments and deletions to accounting records are authorised. Carry out independent checks to ensure amendments have been made correctly. Establish authorisation levels. • Perform frequent independent checks, including spot checks. • Reconcile accounting records and petty cash frequently, maintain reconciliation records and carry out independent reviews, investigate and resolve all discrepancies. • Report any discrepancies that cannot be resolved, or any losses that have occurred. Regularly review suspense accounts to confirm their validity.
Invoices are falsified or duplicated in order to generate false payment.	• Segregate duties between ordering and payment of invoices. Carry out routine checks: • - Invoice has a genuine purchase order number. • - Match invoice to purchase order and goods received note. • - Check invoice detail looks right, that amounts and calculations are correct etc. • - Ensure invoice had not already been paid, by checking relevant records.
Supplier bank account details are changed in order to divert payments.	• Only accept requests for changes to supplier standing data in writing. • Seek confirmation from the supplier that the requested changes are genuine using contact details held on the vendor data file or from previous and legitimate correspondence. Do not contact the supplier via contact details provided on the letter requesting the changes. • Ensure that there is segregation of duties between those who authorise changes and those who make them. • Maintain a suitable audit trail to ensure that a history of all transactions and changes are maintained. • Produce reports of all changes made to supplier standing data and check that the changes were valid and properly authorised before any payments were made. • Regularly verify the correctness of standing data with suppliers.
Unauthorised use of cheques and payable orders	• Hold financial stationery securely and maintain records of stock holdings, withdrawals and destruction of wasted stationery. • Establish signatories and delegated powers for cheques and payable orders. • Reconcile cheques and payable orders to source documentation before issue. • Use restrictive crossings such as “non-transferable” and “a/c payee”. • Ensure that addresses to which payable instruments are sent are correct. For large value payments check encashment to ensure that the intended recipient did receive the payment. • Discover the fraudulent amendment of cheque details by careful choice of inks and printers so that the print produced on cheques is as indelible as possible. • Print the amount in figures as close to the £ as possible. • Write payee details in full rather than use abbreviations or acronyms. • Fill up blank spaces with insignificant characters such as asterisks. • Use envelopes that make it less obvious that they contain cheques for mailing purposes. • Ensure that signed cheques are not returned to payment staff. • Reconcile bank statements with check listings regularly. Check that there are no missing/out of sequence cheque numbers

Payroll/Travel & Subsistence

Risks that may be associated with the payroll function include the introduction of non-existent (ghost) employees, unauthorised amendments made to input data, and the payment of excessive overtime, bonus or travel claims. This section suggests some controls that should be in place.

How fraud could be perpetrated	**Examples of controls**
Creating fictitious employees whose pay is then obtained by the fraudster or by someone in collusion, or obtaining pay that is not consistent with the employee's grade.	• Ensure that only authorised personnel are able to update payroll records. • Segregate duties between those responsible for authorizing appointments and those who make changes to standing data and action payments. • Produce listings of all starters, leavers and changes to standing data as part of every payroll run and check that all changes have been made correctly. • Produce regularly exception reports (eg emergency tax codes for more than 6 months, no NI numbers, duplicate payees), for investigation by management. • Subject the payroll master file to periodic checks by HR to ensure that each post is authorised, that the correct person is in post, that the person exists and that basic salaries and allowances are correct. • Provide budget holders with sufficient and timely information to enable them to reconcile staffing costs against budget.
Making false claims for allowances, travel and subsistence	• Establish a comprehensive set of rules and ensure that they are communicated to staff. Establish a formal process that involves line managers approving and reviewing work plans and programmes for visits, especially for staff where there is no countersigning requirement. • Institute checks by countersigning officers of claims against approved work plans, standard mileages for regular destinations and primary evidence such as hotel bills, rail tickets and taxi receipts. • Instruct finance teams to ensure that correct rates are claimed; substantiating documents (eg hotel invoices) are included and check that authorised claims were received from approved countersigning officers. • Establish random sample management checks to verify details on claims and to ensure that finance team checks were applied rigorously to claims. • Provide budget holders with sufficient information to enable them to monitor costs against budget.
Misuse of Corporate Credit Cards	• Establish clear policy/rules and communicate to all staff. • Make one person or central group responsible for issuing cards (e.g. payments section). Authorise all card issues. • Maintain a record of cardholders. Establish monthly credit limits. • Require cardholders to submit expense claims regularly supported by invoices/receipts to the group that process payments for checking and reconciliation to card issuer statements. • Ensure that cards are returned and destroyed when staff move or cease to be cardholders.

Grant payments

This section sets out examples of the controls that should be in place to counter the fraud risks specifically associated with payment of grants:

How fraud could be perpetrated	Examples of controls
Grant funds are misappropriated	• Establish clear guidelines on claims procedures are communicated to all staff employed to process claims, especially new recruits. • Establish delegated authorities and levels of authorisation • Assess claims to determine their complexity and level of risk and allocate accordingly to officers with the relevant experience and expertise. • Check all claims and supporting evidence for accuracy, completeness and timeliness. • Maintain good segregation of duties throughout the process (eg approval, processing, payment authorisation, payment). • Maintain good quality case records. • Assess training needs periodically and draw up appropriate training plans. • Check claims by individuals to previous claims to reduce the risk of duplicating payments. • Carry out periodic reassessments on on-going claims. • Liaise with other grant making organisations to reduce the risk of making payments where the payment of other grants mean that claimants are not entitled to them. • Scrutinise reports of grant payments regularly to ensure that only approved grants have been paid out and that they have gone to the correct recipients. • Review systems operated by organisations who receive grant funding for specific projects to ensure that the spending of grant monies is adequately controlled.

Contracting

The section sets out some examples of controls which should be in place, in addition to those which apply generally to cash handling and purchasing systems, to counter the fraud risks faced in relation to the use of contractors.

How fraud could be perpetrated	Examples of controls
A contractor could be selected as a result of favouritism or who does not offer best value for money	• Draw up and agree a clear and comprehensive specification. • Use a Central of Procurement Expertise to carry out the tendering and letting procedures. Comply with Procurement Guidance Notes. • Seek tenders from suitable suppliers (must comply with EC/GATT regulations). Draw up clear and comprehensive tender evaluation criteria. • Arrange for tenders to be delivered to those responsible for selection without interference. Do not accept late tenders. • Ensure that tenders are evaluated against the agreed evaluation criteria by a tender evaluation board. • The Project Board should approve the successful contractor. • Require staff to declare any personal interests they may have which may affect the tendering process.

Payments made for work not carried out as a result of collusion between contractor and official	• Ensure that invoices are supported by independent certification that work was performed satisfactorily before authorising payment. • Maintain a register of contracts in progress. • Only add approved and authorised contracts to the register. Accept invoices from approved contractors only. • Ensure that all contract variations are supported by sequentially numbered and • authorised variation orders before payment.

Purchasing

Risks associated with the operation of purchasing systems include the false input of invoices, the diversion of payments and misappropriation of purchases. This section sets out some examples of controls that should be in place to reduce the risk of fraud in this area:

How fraud could be perpetrated	**Examples of controls**
Unauthorised use of purchasing systems in order to misappropriate goods or use services for personal gain.	• Restrict opportunity to generate payment by using sequentially numbered purchase order forms for all orders; perform independent checks to show that purchase orders are valid and accounted for. • Establish authorised signatories and authorisation limits for requisitioning and placing orders. • Match invoices with orders before the invoice is certified for payment. • Keep stock records up to date so that stocks, stock usage and orders can be monitored. • Separate the duties between those ordering, receiving goods, and approving and paying invoices. This separation of duties should be reviewed regularly. • Ensure that authorised staff make amendments to standing data (e.g. supplier records). • Provide budget holders with sufficient and timely information to enable them to reconcile expenditure against budget.
Short deliveries of goods or services	• Check delivery notes to original orders, chase up short deliveries, and only pay for goods received.
Acceptance of unsolicited goods or expanded orders as a result of fraudulent acceptance of attractions such as free gifts.	• Confirm goods were properly ordered, authorised and received before authorising payment. • Only pay for goods ordered.
Misuse of Government Procurement Cards (GPC)	• Establish a clear GPC policy that is communicated to all staff and should include expenditure limits for individual transactions. • Appoint an individual to be the cardholder manager who will be responsible for appointing cardholders and for dealing with the card issuing bank. • Maintain a list of authorised cardholders. • Cardholders should maintain a log of all transactions that should be supported by authorisations to make purchases, invoices/receipts. • Cardholders must hold cards securely. • Cardholders must check all entries on statements supplied by the bank and refer any discrepancies to the cardholder manager. • Budget holders should carry out periodic checks to ensure that GPC statements are properly reconciled and that only authorised purchases are made. • Ensure that cards are returned to the cardholder manager and

	cancelled with the bank when cardholders move or cease to be cardholders. The cardholder manager should also ensure that the card is destroyed and the record of cardholders amended.
Orders placed on the Internet are not delivered or goods received are not of the desired quality	• Make sure your browser is set to the highest level of security notification and monitoring. • Check that you are using the most up to date version of your browser and ensure their security features are activated. • Keep a record of the retailer's contact details, including a street address and non-mobile telephone number. Beware if these details are not available on the website. Do not rely on the e-mail address alone. • Click on the security icon to see if the retailer has an encryption certificate. This should explain the type and extent of security and encryption it uses. Only use companies that have an encryption certificate and use secure transaction technology. • If you have any queries or concerns, telephone the company before giving them your card details to reassure yourself that the company is legitimate. • Print out your order and consider keeping copies of the retailer's terms and conditions and returns policy. Be aware that there may well be additional charges such as postage and VAT, particularly if you are purchasing goods from traders abroad. When buying from overseas always err on the side of caution and remember that it may be difficult to seek redress if a problem arises. • Check statements from your bank or card issuer carefully as soon as you receive them. Raise any discrepancies with the retailer concerned in the first instance. If you find any transaction on your statement that you are certain you did not make, contact your card issuer immediately. • Check that you are fully aware of any payment commitments you are entering into, including whether you are instructing a single payment or a series of payments. • Never disclose your card's PIN to anyone, including people claiming to be from your bank or the Police, and NEVER write it down or send it over the internet. • If you have any doubts about giving your card details, find another method of payment.

Assets

Risks in this area include use of assets for personal gain, or misappropriation of assets. This section suggests some controls that should be in place to counter those risks.

How fraud could be perpetrated	**Examples of controls**
Theft or unauthorised use of assets	• Maintain up to date asset registers and inventories • Ensure that assets are assigned to individual budget centres. • Clearly describe assets in registers and inventories. • Mark assets in some way (e.g. property of xxx). • Store assets securely. • Carry out regular spot checks to confirm existence of assets.

Information

The final section deals with some of the controls that should be in place to reduce the threat of fraud or other irregularities arising from access to sensitive information or misuse of information for private gain.

How fraud could be perpetrated	Examples of controls
Theft of sensitive/restricted documentation or information	• Identify all information assets. • Produce a clear information risk policy and communicate to all staff. • Implement the Government Mandatory Minimum Measures for managing information risk. • Define key roles and responsibilities for managing information risk (e.g. Senior Information Risk Owner, Information Asset Owners) and allocate to named individuals. • Establish an effective information risk governance framework. • Ensure that data security arrangements are underpinned by a culture that values and protects data. • Carry out regular assessments of the information risks and whenever changes occur to technology or new threats are identified. • Restrict access to information on a need to know basis. • Ensure that access rights are reviewed regularly and that these are removed for staff that leave. • Limit the use of removable media (eg laptops, USB memory sticks, CDs). Encrypt data transferred to removable media. • Do not use e-mail to transmit confidential information unless it is encrypted. • Regularly check the activities of those with rights to transfer personal or sensitive data to ensure that they continue to have a business case for these activities. • Ensure that all data users successfully undergo information-risk awareness training. • Ensure that contingency arrangements (so that damaged or lost data can be renewed or replenished quickly) are regularly tested. • Put in place arrangements to log activities of data users and for managers to review usage. Computer logs should be adequately protected against unauthorised access and amendment.

Money laundering

While most public bodies are not regulated under the Money Laundering Regulations, bodies could be at risk from criminals using the organisation's systems to launder cash gained through involvement in criminal activities.

How fraud could be perpetrated	Examples of controls
Individuals or groups pass money transactions through organisational systems	• Carry out assessment of the risk the organisation is at from being used to launder "dirty cash". • Depending on the outcome of such an assessment controls can include: • Developing anti money laundering policies and processes. • Appoint a Money Laundering Reporting Officer. • Provide awareness training to staff. • The Joint Money Laundering Steering Guidance approved by HMT may be a useful source of information in this area.

Appendix 3 - 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.

Internal Control

"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. This threat may increase with the introduction of systems designed to meet current and future Government targets (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 also has the potential to cause major disruption, significant financial loss or even serious reputational damage 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.

These 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 ***Appendix 2.***

The "Fear Factor"

Major deterrents to perpetrating fraud are the risk of being caught and the severity of the consequences. The most important fact about deterrence is that it derives from *perceived* risk and not *actual* risk. Organisations may manage to increase the actual risk of detection but it will only achieve a deterrent effect if it ensures that *perceptions* of risk change too. Ways in which organisations can do this include:

- Warnings on forms such as: "false statements may lead to prosecution";
- General publicity;
- Increasing the severity of penalties; and
- Always taking appropriate action against known perpetrators of fraud.

Changing Attitudes to Fraud

The most effective strategies designed to change attitudes rely on motivation rather than fear. They aim to persuade people of the undesirability of a particular behaviour. Attitude changing strategies rely to a large extent on publicity campaigns to achieve their effect so it is important that departments carry out a full appraisal of the benefits of any proposed advertising campaign and to establish some way of measuring the outcomes of such campaigns. Organisations need to be clear about the objectives and targets of their campaigns.

Appendix 4 - DoF RAISING CONCERNS (WHISTLEBLOWING) OPERATIONAL ARRANGEMENTS

All of us at some point may have concerns about what is happening at work. However, when it is about unlawful conduct, a possible fraud or a danger to the public or the environment, or other serious malpractice, it can be difficult to know what to do.

You may have worried about raising such a concern and may have thought it best to keep it to yourself, perhaps feeling it was only a suspicion. You may have felt that raising the matter would be disloyal to colleagues, managers or to DoF. You may have decided to say something but found that you have spoken to the wrong person or raised the issue in the wrong way and were not sure what to do next.

DoF has put in place a new Raising Concerns (Whistleblowing) arrangements to reassure you that it is safe and acceptable to speak up. They also enable you to raise any concern about malpractice at an early stage and in the right way. If something is troubling you which you think we should know about or look into, these arrangements set out the steps you should take and identify the key contacts, and our assurances to you.

We are committed to making raising a concern work. If you raise a genuine concern under these arrangements, you will not be at risk of losing your job or suffering any form of retribution as a result. Provided you are acting in good faith, it does not matter if you are mistaken. While we cannot guarantee that we will respond to all matters in the way that you might wish, we will strive to handle the matter fairly and properly. By using these Raising Concerns arrangements you will help us to achieve this.

A copy of the Department's DoF Raising Concern Operational Arrangements is available on the Department’s website.

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:	*[Insert name of business area]*
Fraud Risk Assessment of:	*[Insert a description of the area being assessed e.g branch, process, type and value of transactions, nature of expenditure, any risks realised, any internal audit or external audit recommendations or concerns.*
Assessment completed by:	*[Insert name of officer completing the assessment]*
Assessment reviewed and agreed by:	*[Insert name of line manager reviewing and agreeing the assessment]*
Assessment agreed on:	*[Insert date assessment is agreed]*
Next assessment due on:	*[Insert date for completion of next fraud assessment]*

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.

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**);

   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 Finance Director annually. Review internally on a regular basis – at least every 6 months.

Appendix 6 - SUMMARY OF GOOD PRACTICE GUIDANCE ISSUED BY THE NICS FRAUD FORUM: COMMUNICATING WITH THE ORGANISATION

This guidance was developed to encourage the promotion of anti-fraud cultures within individual organisations. Examples of how this can be done include:

All Employees

- Establishing a short focused fraud awareness training programme which includes organisational whistle blowing arrangements, and ensure all staff attend it.
- Making the anti-fraud policy and fraud response plan available to all staff. This should be done via networked IT systems with an e-mail notification supported by the Accounting Officer.

Regular Updates

- Key changes to fraud policy/response plans being communicated immediately to staff via networked IT systems.
- Reporting to staff and publicising the outcomes of fraud investigations and the disciplinary action/prosecutions against employees who perpetrate theft or fraud. Consider including these issues in the organisation's newsletter or website.

Other communication tools that can be used include:

- desk aids given to staff;
- information leaflets or booklets produced for staff;
- displaying anti fraud posters; and
- running fraud awareness roadshows.

Appendix 7 - CONTACT DETAILS

Name	Designation	Telephone Number
Stewart Barnes	Finance Director	9025 4723 (Ext 54723)
Brenda Crummy	Head of Corporate Governance Branch, Finance Division (Deputy for Finance Director)	9081 9645 (Ext 37645)
Velma Beacom	Deputy for Head of Corporate Governance Branch, Finance Division	9045 5700 (Ext 72700)
Lacey Walker	Head of Internal Audit	9037 8603 (Ext 88603)