PUBLIC PROSECUTION SERVICE FOR NORTHERN IRELAND

ANTI-FRAUD POLICY & FRAUD RESPONSE PLAN

Final – v 1.7 – August 2016

CONTENTS

PUBLIC PROSECUTION SERVICE (PPS)

ANTI-FRAUD POLICY

Introduction

1. There is a continuing need to raise staff awareness of their responsibility to safeguard public resources against the risk of fraud. The overall purpose of this Anti-Fraud Policy is to detail the actions we must take and the responsibilities we have regarding the prevention of fraud. The procedures to be followed in the event of a fraud, attempted fraud or irregular activity being suspected are detailed in the Fraud Response Plan. Both documents relate to fraud and loss within the Department.

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. Accordingly, PPS 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.

Definition

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

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

Department's Responsibilities

9. 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) page of the Department of Finance (DoF) website: Accountability and Financial Management / DoF. AFMD also publishes the NICS Annual Fraud Report.

10. 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.

11. Overall responsibility for managing the risk of fraud has been delegated to the **Senior Assistant Director, Resources and Change**[1] whose responsibilities include:

    (a) Developing the Department's Fraud Risk Register and undertaking a regular review of the corporate fraud risk assessments in order to keep the register current (page 16 refers).

[1] In practice the majority of duties will be delegated to the Head of Finance under the oversight of the SAD or other key staff

(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 fraud risk;

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

(e) Advising the Assistant Directors / Heads of Business on the conduct of fraud investigations and liaising where necessary with the NICS Group Fraud Investigation Service (GFIS), the Head of Human Resources and the Head of Internal Audit in accordance with the Fraud Response Plan.

(f) 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 / Assistant Director who must then report to Head of Finance, and Head of Human Resources.
- Reporting externally to AFMD and the Comptroller and Auditor General, Northern Ireland Audit Office (NIAO) in accordance with MPMNI Annex 4.7; and
- Coordinating assurances about the effectiveness of anti-fraud policy and fraud response plan to support the Governance Statement;

(g) Liaising with the PPS Audit and Risk Committee;

(h) Making sure that all staff are aware of the organisation's Anti-Fraud Policy and Fraud Response Plan and that they know what their responsibilities are in relation to combating fraud;

(i) Ensuring that appropriate action is taken to minimise the risk of similar frauds occurring in future;

(j) Ensuring that appropriate pre-employment screening measures are undertaken;

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

(l) Ensuring that vigorous and prompt investigations are carried out if fraud occurs, is attempted or is suspected;

(m) Ensuring that advice and support is provided to management in implementing suspensions and any subsequent disciplinary investigation, including advising on the application of the NICS Disciplinary Policy;

(n) Ensuring, where appropriate, legal and/or disciplinary action is taken against perpetrators of fraud;

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

(p) Ensuring, where appropriate, disciplinary action against staff who fail to report fraud; and

(q) Taking appropriate action to recover assets and losses.

Responsibilities of all Assistant Directors / Heads of Branch include:

12. (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 Head of Finance as soon as they become aware of such instances;

(g) Where appropriate overseeing the conduct of fraud investigations and liaising where necessary with the Head of Finance 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.

Line Managers' Responsibilities

13. 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**.

14. 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 a 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 extent 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.

15. 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.

16. 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.

Staff Responsibilities

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

(a) 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;

(b) 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

(c) 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.**

18. It is the **responsibility** of every member of staff to report details immediately to their line manager / Head of Branch / Assistant Director who will then report to the Head of Finance if they suspect that a fraud has been attempted or committed, or have seen any suspicious acts or events. More details on reporting are included in the Department's **Fraud Response Plan** within this document. The Public Interest Disclosure (NI) Order 1998 – see CSC 04/03 Guidance on Public Interest Disclosure ('whistleblowing') – protects the rights of staff who report wrongdoing. If you are in any doubt, you should speak to your line manager or their immediate manager, the Head of Finance, Head of Human Resources or the Senior Assistant Director, Resources and Change. A PPS Whistleblowing Policy has been developed and can be found on the PPS Intranet. Information is also available in **Appendix 4**.

19. 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)

20. Advice is also available through the independent charity Public Concern at Work on **020 7404 6609** or by email at **whistle@pcaw.org.uk**. Their lawyers can give free confidential advice at any stage regarding a concern about serious malpractice at work. For more information, you can visit their website at www.pcaw.org.uk. An

employee can, of course, also seek advice from a lawyer of their own choice, at their own expense.

21. 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 (page 20).**

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

23. 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 within the Corporate Management / Corporate Governance section on the PPS Intranet and website.

24. 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.

Internal Audit

25. 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.

26. 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 create the opportunity for 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.

27. The Head of Finance / the Head of Human Resources 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. They may draw on the Internal Audit function to do so. All cases of suspected or actual fraud should be reported immediately to the Head of Finance.

Account NI

28. The purpose of Account NI is to provide an integrated Resource Accounting and Budgeting System for all NICS Departments. PPS joined Account NI on 2 July 2012.

29. The handling process for suspected, attempted or actual frauds detected by Account NI is as follows:

- Account NI will immediately report any suspected, attempted or actual frauds detected to the Finance Director of the department where the potential or actual financial loss lies (the “relevant department”). In accordance with the DoF anti-fraud policy and fraud response plan these reports will also be copied to the Head of Internal Audit, the Head of Human Resources and DoF.

- The relevant department will notify these incidents to the Comptroller Auditor General (C&AG) and AFMD where applicable in line with their own anti-fraud policies.

- The suspected fraud will be dealt with in line with the relevant department's policies. Account NI will assist with the investigation where possible including the identification and communication of implications (if any) for other user Departments.

- It is expected that the relevant department will continue to monitor and report on the case under their own procedures.

- This means that all cases will be reported to the C&AG and AFMD by a single department and it is clear that the responsibility for fraud investigation and reporting lies with the relevant department.

- Departments will ensure that any changes to procedures recommended as part of any fraud investigation are discussed with Account NI in order that any appropriate changes can be made to Account NI processes.

Fraud Investigation

30. 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.

31. It is departmental policy that there will be consistent handling of all suspected fraud cases without regard to position held or length of service.

32. Investigators should have free access to all staff, records and premises in order to carry out investigations.

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

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

IF IN DOUBT, ASK FOR ADVICE.

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

Group Fraud Investigation Service (GFIS)

36. 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, Michelle Anderson and is based at Annex C Dundonald House, Stormont Estate, Belfast. The contact number is 028 90 544210 or ext 24410.

37. The GFIS provides fraud investigation services to the Department in line with a Service Level Agreement agreed between GFIS and the Department.

38. The GFIS 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 **Head of Finance** in the first instance.

PPS Fraud Working Group

39. The PPS Fraud Working Group provides a strategic overview of counter fraud activities within the PPS. In particular the Group has the following remit:

- Monitor and review, and disseminate as necessary, outputs of the NICS Fraud Forum;
- Co-ordinate 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 PPS 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.

40. The Group is chaired by the Senior Assistant Director, Resources and Change and is attended by the Head of Finance, Head of Human Resources (or their representatives), Head of Central Management Unit, Head of Business Assurance, a representative from PPS Fraud and Departmental Section and the PPS representative on the NICS Fraud Forum. Membership is flexible and may include other parties as the occasion demands.

41. The Fraud Working Group meets at least twice per year and is scheduled to follow the NICS Fraud Forum meetings. The Audit and Risk Committee and the People and Resources Committee are advised of discussions and activities undertaken by the Group.

National Fraud Initiative

42. 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

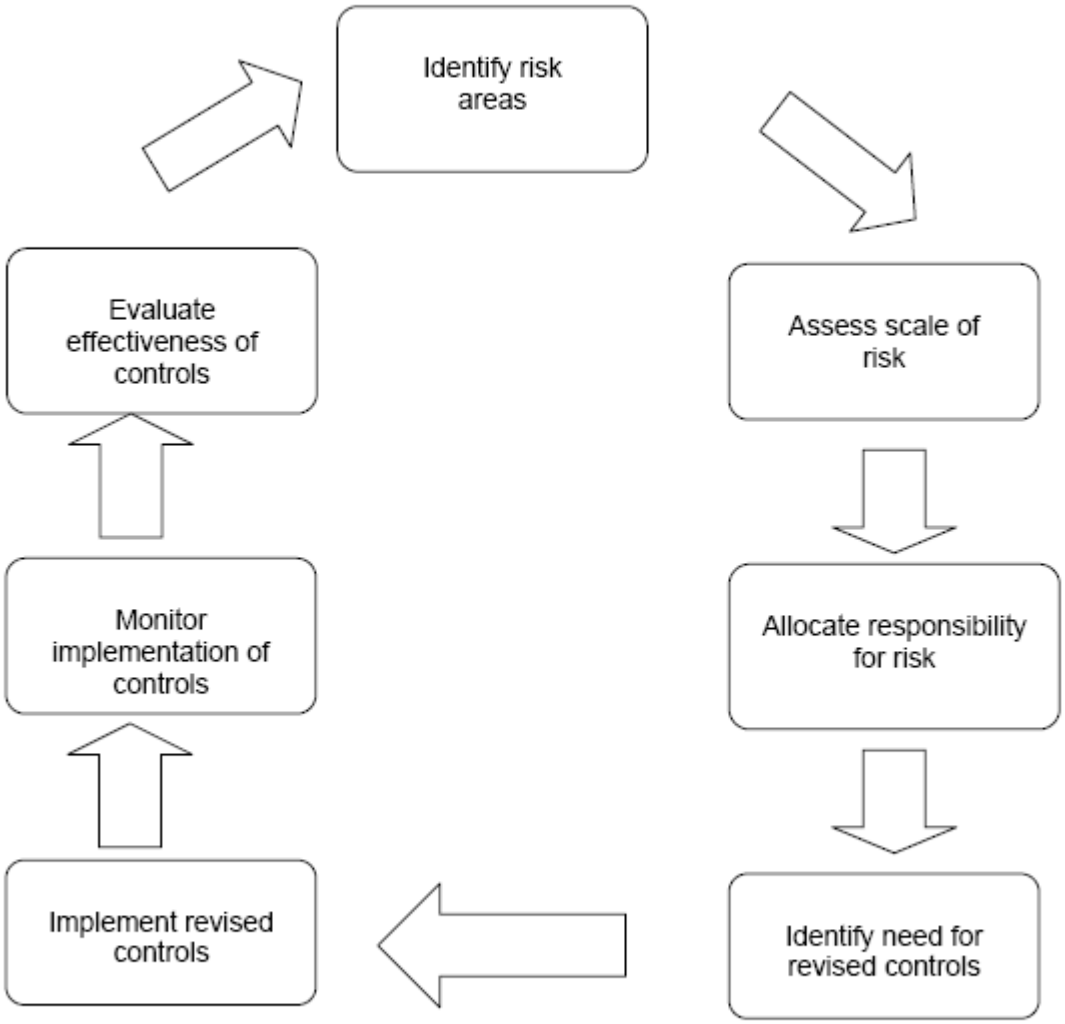
exercises, requesting data from a range of public bodies, for the purposes of assisting in the prevention and detection of fraud.

43. The Department participates in the NFI exercise providing payroll, pensions, trade creditors, housing benefit, rate relief and domestic rates data, and sets to successfully identify cases of suspected fraud and overpayments. Participation in the NFI represents a key strand of the Department's anti-fraud policy.

Fraud Risk Assessments

44. 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. The diagram below sets out the key stages of a risk management cycle to help deal with fraud. Please see **Appendix 6** – Guidance on Performing an Assessment of Fraud Risks.

RISK ASSESSMENT CYCLE



Disciplinary Action

45. 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 fraudulent act will be considered to have committed a serious disciplinary offence, and is likely to be dismissed from the Department on the grounds of gross misconduct.

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

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

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

Malicious Allegations

49. 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.

Conclusion

50. 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.

51. Any queries in connection with this policy document should be directed to the Head of Finance and/or the Head of Human Resources.

52. Current contact details are provided in **Appendix 5**.

PUBLIC PROSECUTION SERVICE (PPS)

FRAUD RESPONSE PLAN

INTRODUCTION

1. The Department has prepared this Fraud Response Plan to act as a procedural guide and provide a checklist of the required actions, which **MUST** be followed, in the event of a fraud, attempted fraud or irregular activity being suspected.

2. Adherence to the Fraud Response Plan will enable the Department to:

   - Take timely and effective action to prevent further losses;
   - Help to recover losses;
   - Establish and secure evidence necessary for possible criminal and disciplinary action;
   - Comply with the external reporting requirements set out in Managing Public Money NI (MPMNI) ; and
   - Highlight areas of weakness in the operating systems to prevent future losses.

3. The overarching theme of this plan is:

   'IF IN DOUBT, ASK FOR ADVICE'

   This applies at any point in an investigation. Details of contacts are provided at **Appendix 5.**

4. A Service Level Agreement has been agreed with the GFIS. This will ensure the completion of investigations in compliance with the necessary legislative framework (e.g. the requirements of the Police and Criminal Evidence (Northern Ireland) Order 1989), professional standards and recognised best practice.

5. A Memorandum of Understanding (MoU) has also been agreed with the Police Service of Northern Ireland (PSNI) for the Public Sector. The MoU provides a basic framework for the working relationships between the NI Public Sector and the PSNI in respect of the investigation and prosecution of suspected fraud cases

6. The following sections of this paper set out the initial steps to take in the event of fraud or suspected fraud:

- Initial Reporting
- Initial Enquiries / Fact Finding
- Management Action
- Formal Notification; and
- Commencement of Investigation

7. **Appendix 7** also provides advice on best practice for reporting suspicions of fraud and irregularity. A high level flowchart setting out the key steps in the preliminary enquiry and formal reporting stages is outlined at **page 32.**

STAGE 1 – INITIAL REPORTING

8. **Action Required by a Staff Member on Becoming Aware of Fraud**

When any member of staff becomes aware of a fraud (whether they discover it themselves or it is reported to them by a third party), they must **orally** notify their line manager / Head of Branch / Assistant Director promptly. If it is not appropriate to raise the concern with their line manager or senior line management, the matter should be brought directly to the attention of the Head of Finance.

9. The Department has a 'Whistleblowing' Policy to assure staff and members of the public that it is safe to speak up if they are concerned about something. In addition, advice is available through the independent charity Public Concern at Work on **02074046609**. 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.

10. **Action Required by Management to whom the Case is Reported**

The line manager / Head of Branch / Assistant Director must report to the Head of Finance. Where a line manager is reporting directly to the Head of Finance they should ensure that the Head of Branch / Assistant Director of their business area is copied into all correspondence unless these individuals appear to be involved or linked with the case.

11. Line management **should not** undertake preliminary enquiries until any suspicion has been reported to and advice taken from Head of Finance. **It is imperative that enquiries should not prejudice subsequent investigations or corrupt evidence, therefore**, **IF IN DOUBT, ASK FOR ADVICE.**

STAGE 2 – INITIAL ENQUIRIES / FACT FINDING

12. The Head of Finance, in conjunction with the Head of Internal Audit and the Head of Human Resources will advise on an initial fact-finding exercise.

13. For significant / novel cases the Head of Finance may establish a Fraud Investigation Oversight Group (FIOG). This will normally comprise of a subset of the PPS Fraud Working Group. Membership in most instances will be the SAD Resources and Change, Heads of Finance, HR and CMU, the Head of Internal Audit and appropriate representation from the business area. Expert advice (e.g. GFIS, DSO) may be sought as necessary.

14. Where the suspected fraud is cross-departmental the FIOG should reflect this and it is recommended that the existing Finance Director network is utilised for this purpose. Where PPS is the lead department in any investigation the Head of Finance will take the lead role in contacting appropriate colleagues to convene a FIOG meeting. The appropriate attendees will be driven by those departments impacted by the case under investigation.

15. The business area must then make arrangements for the necessary initial enquiries to be made and the facts gathered to confirm that a fraud is suspected or proven. Depending on the nature and scale of the case and the information requirements, these responsibilities may be delegated to an official at an appropriate level within their business area, for example, for lower level / less complex cases.

16. This discreet preliminary enquiry should be carried out as speedily as possible (normally within 5 working days) after the suspicion is raised and with due consideration to potential future prosecutions and the need to ensure evidence is not compromised. The purpose of the initial fact-finding exercise is to determine the factors that gave rise to suspicion and to clarify whether a genuine mistake has been made or it if it likely that a fraud has been attempted or occurred. This may involve enquiries with staff or the examination of documents.

STAGE 3 – MANAGEMENT ACTION & STAGE 4 – FORMAL NOTIFICATION

17. If the initial enquiries confirm that a fraud has not been attempted or perpetrated, no further action is necessary apart from documenting the outcome of the initial enquiry. The exception would be if there are issues concerning non-compliance with NICS Code of Ethics, and such cases should be reported to the SAD Resources and Change. In addition, if internal controls were found to be deficient, management should review their control systems with a view to ensuring they are adequate and effective.

18. **Action to be taken when the Initial Enquiries Confirm a Suspicion of Fraud in or against the Department**

If the initial enquiries confirm the suspicion of fraud, management must ensure that all original documentation is preserved in a safe manner for further investigation. This is to prevent the loss of evidence, which may be essential to support subsequent disciplinary action or prosecution.

19. **Formal Notification of the Case**

Using the template at **Appendix 8** the business area contact should report the facts immediately, **internally**, to the:

- Assistant Director (for those members of staff working in the regions or headquarters sections);
- Head of Branch (for Corporate Services staff); and, in all cases to:
- Head of Finance

20. The Head of Finance is responsible for the **external** reporting of all discovered fraud, proven or suspected, including attempted fraud, within or against the Department to:

- the Comptroller and Auditor General (C&AG), Northern Ireland Audit Office (NIAO); and
- Accountability and Financial Management Division (AFMD) of DoF.

21. C&AG should be promptly notified of new fraud cases. Stage 1(Initial Reporting) to Stage 4 (Formal Notification) should normally be completed within 10 working days. To enable the Head of Finance to meet this timescale, business areas should normally forward **Appendix 8** to the Head of Finance within 8 working days of the matter being initially reported.

22. The Head of Finance will ensure that updates on progress regarding the completion of investigations are provided to NIAO and AFMD as necessary, to meet external reporting requirements. Care will be taken in making such reports that potential future legal proceeds are not jeopardised.

23. To remove any threat of further fraud or loss, management should immediately change/strengthen procedures and if appropriate, suspend any further payments pending full investigation. Where the fraud has been perpetrated externally management should consider the need to inform other government departments / bodies.

24. Reporting arrangements apply to **all monies for which the Department is accountable.**

25. The Head of Finance will complete the Department's annual fraud return to AFMD and provide regular updates to the PPS Audit and Risk Committee and Management Board.

STAGE 5 - INVESTIGATION

26. The Head of Finance, in conjunction with the Head of Human Resources and Head of Internal Audit, will decide on the appropriate course of action including the full formal investigation arrangements (e.g. whether or not a case should be referred to GFIS), and will be responsible for reporting to and liaison with the Accounting Officer, Senior Assistant Director, Resources and Change, Chair of the Audit and Risk Committee, as necessary. The Head of Finance will notify NIAO and AFMD.

27. If appropriate, the Head of Finance will establish a FIOG to determine the scope of the investigation. This will normally comprise of a subset of the Fraud Working Group. Membership in most instances will be the SAD Resources and Change, as Senior Responsible Officer (SRO), Heads of Finance, HR and CMU, the Head of Internal Audit, appropriate representation from the business area and GFIS. Expert advice (e.g. Forensic accountants, DSO) may be sought as necessary.

28. The SRO will appoint a Case Manager, normally from within the relevant business area to manage and control the investigation. The Case Manager will have no conflict of interest, be of appropriately senior grade and have proportionate knowledge and skills to manage the case.

29. The SRO's main role is to oversee the conduct of an effective investigation, undertaken in a timely manner. They will have overall responsibility and accountability for the independence and integrity of the investigation. On this basis they are responsible for:

- identifying the expected level of fraud investigation resources required;

- making sufficient resources available to fund this requirement from GFIS;
- liaising at an early stage with GFIS on suspected cases;
- providing access to all records, assets, personnel and premises, and with the authority to obtain such information and explanations as are considered necessary to fulfil fraud investigation responsibilities;
- ensuring that evidence (including computer files and records of amendments relevant to the case) gathered during initial fact finding is not compromised. Evidence and records should be protected and preserved for future consideration during a detailed investigation. In addition, they should not be disposed of under the normal review process;
- liaising with GFIS Investigators to determine the need for an investigation and the required scope of such investigations;
- approving the Terms of Reference and Investigation Plan produced by GFIS;
- where appropriate establishing a FIOG or other Client oversight mechanisms;
- co-ordinating meetings of FIOG where applicable, and producing accurate and timely minutes of meetings;
- at a corporate level overseeing the fraud investigation being undertaken within their organisation by GFIS staff;
- taking key management decisions in fraud investigation cases, based on advice/recommendations from GFIS staff e.g. on police referral, recovery options;
- documenting any decision not to investigate a particular aspect of the allegation;
- fully engaging with GFIS staff throughout investigations, including providing free and unfettered direct access to the Accounting Officer, Audit Committee Chair and other senior managers where required;
- where required supporting the utilisation of Internal Audit staff to assist GFIS staff undertaking investigations;
- taking appropriate corrective action to address weaknesses or lessons learned as highlighted by investigations;
- continuing to provide departmental representation at the NICS Fraud Forum;
- ensuring that any key cross cutting lessons learned and patterns with previous cases for consideration are highlighted and key messages disseminated appropriately;

- liaising as appropriate with the officer responsible for exercising disciplinary powers and ensuring that the independence of their role and the integrity of the disciplinary process is not compromised; and
- liaising with senior management so recovery and disciplinary actions are addressed and controls are improved. For investigations conducted under disciplinary procedures, the Head of HR will initiate disciplinary action.

30. In most cases the SRO will decide to delegate some of the roles set out above (e.g. to the Head of Finance) but always retaining SRO responsibility.

31. If GFIS are involved they will be responsible for:

- attending case conferences with the Client to discuss initial information/allegations/concerns;
- assisting the Client in assessing the need for a preliminary/full investigation to be undertaken;
- developing the Terms of Reference and investigation plan for individual cases being investigated in line with the scope agreed with the Client/department carrying out required investigatory work;
- reporting at key points to the relevant Client on progress and findings;
- providing advice/recommendations to the Client on the appropriate actions to be taken e.g. referral to police, recovery options etc;
- liaising with PSNI, PPS, Forensic Science and other specialists as required;
- producing evidence packs for PSNI investigation or the preparation of prosecution files for PPS decision;
- attendance at court/tribunal hearings etc;
- where required working with departmental Internal Audit teams and other specialists in the investigation of fraud cases;
- maintaining professionally qualified investigatory team of staff to undertake investigations;
- liaising with Clients in respect of any PR/media issues;
- providing feedback on lessons learned from investigations e.g. procedural/ legislative weaknesses;

- liaison with Departmental HR (DHR) in respect of cases involving employees; and
- subject to availability of resources, the provision of fraud awareness seminars.

32. Independence and the perception of independence in the conduct of all fraud investigations are paramount. Whilst the investigation may be conducted by officials or senior management within the affected business area, there should be no reasonable link (i.e. a conflict of interest) between investigating personnel, including the SRO, and the fraud case. The independence and integrity of the investigation and the investigating personnel must be kept under review throughout the process.

33. For any significant and potentially complex cases a SRO may be appointed by the Director. In such cases consideration should be given to the need for the investigation to be conducted independently from the Department.

34. An internal investigation can, of course be taken forward under established disciplinary procedures by staff in DHR. Where cases involving disciplinary procedures do not merit the oversight of a SRO, their role will not infringe upon the independence of the officer responsible for exercising disciplinary powers.

LIAISON WITH THE POLICE SERVICE OF NORTHERN IRELAND

35. It is departmental policy that in **cases of fraud**, whether perpetrated or attempted by a member of staff or by external organisations or persons, the case will be referred to the PSNI, as necessary, at the earliest possible juncture. For example, in a case involving the theft of an asset, the police will be contacted upon discovery of the theft whereas in cases such as abuse of flexible working hours, police involvement may not be deemed necessary.

36. The Head of Finance should ensure that legal and/or police advice is sought where necessary. GFIS, on behalf of the Head of Finance, will lead on liaisons with the PSNI in accordance with the operating protocols set out in the Memorandum of Understanding (MOU) with the PSNI. Initial contact with GFIS should be through the Head of Finance.

37. The MOU sets out a framework to ensure appropriate action is taken by public sector organisations in line with DoF guidelines to deal with cases of suspected, attempted or actual fraud. It also aims to ensure that, where specifically appropriate, actions throughout the investigative process are conducted in accordance with the Police and Criminal Evidence (Northern Ireland) Order 1989 (PACE). Where investigations are required to be conducted in accordance with PACE a trained official will advise on the specific requirements.

38. If the police decide to investigate then it may be necessary for the Head of Finance to postpone further internal action. Where this is the case then this course of action should be formally documented and the Head of Finance should continue to liaise with the police at regular intervals and if required report on progress to senior management.

SANCTION AND REDRESS

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

40. There are three main actions that the Department may pursue as part of its fraud investigation:

    a. Conduct the investigation to a criminal standard to maximise the opportunities for a criminal investigation. This course of action may include the preparation and submission to the PSNI of an evidential pack. Alternatively, where in-house expertise is available, the investigation can be taken forward with a view to presenting a file to the Public Prosecution Service for decision;
    b. Seek redress of any outstanding financial loss through the Civil Courts, if appropriate; and
    c. Pursue the internal disciplinary process which may, if there is clear evidence of supervisory failures, include other officials.

41. Each option needs careful consideration in order to decide on the most appropriate course of action to be taken in each case. It is important any civil/disciplinary action does not impair a criminal investigation and vice versa.

42. Where sufficient evidence is available to allow prosecution the independence of the decision making prosecutor must be assured.

POST EVENT ACTION

43. 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 fraud will not recur. Additionally, if a departmental employee is suspected of involvement, the Head of Human Resources will consider the appropriate course of action. This may range from close monitoring / supervision to precautionary suspension, however, it should be noted that suspension does not in any way imply guilt.

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

COMMUNICATION

45. The following communications should be observed in all cases:

- The PPS Audit and Risk Committee (ARC) should be kept informed;
- This Departmental **Fraud Response Plan** should be reviewed to determine whether it needs to be updated and if so, changes should be circulated throughout the organisation;
- Where the allegation has been made by a Whistleblower or individual (and their identify is known), the SRO or Case Manager should provide regular and proactive feedback on the progress of the investigations, as set out in the Whistleblowing guidance;

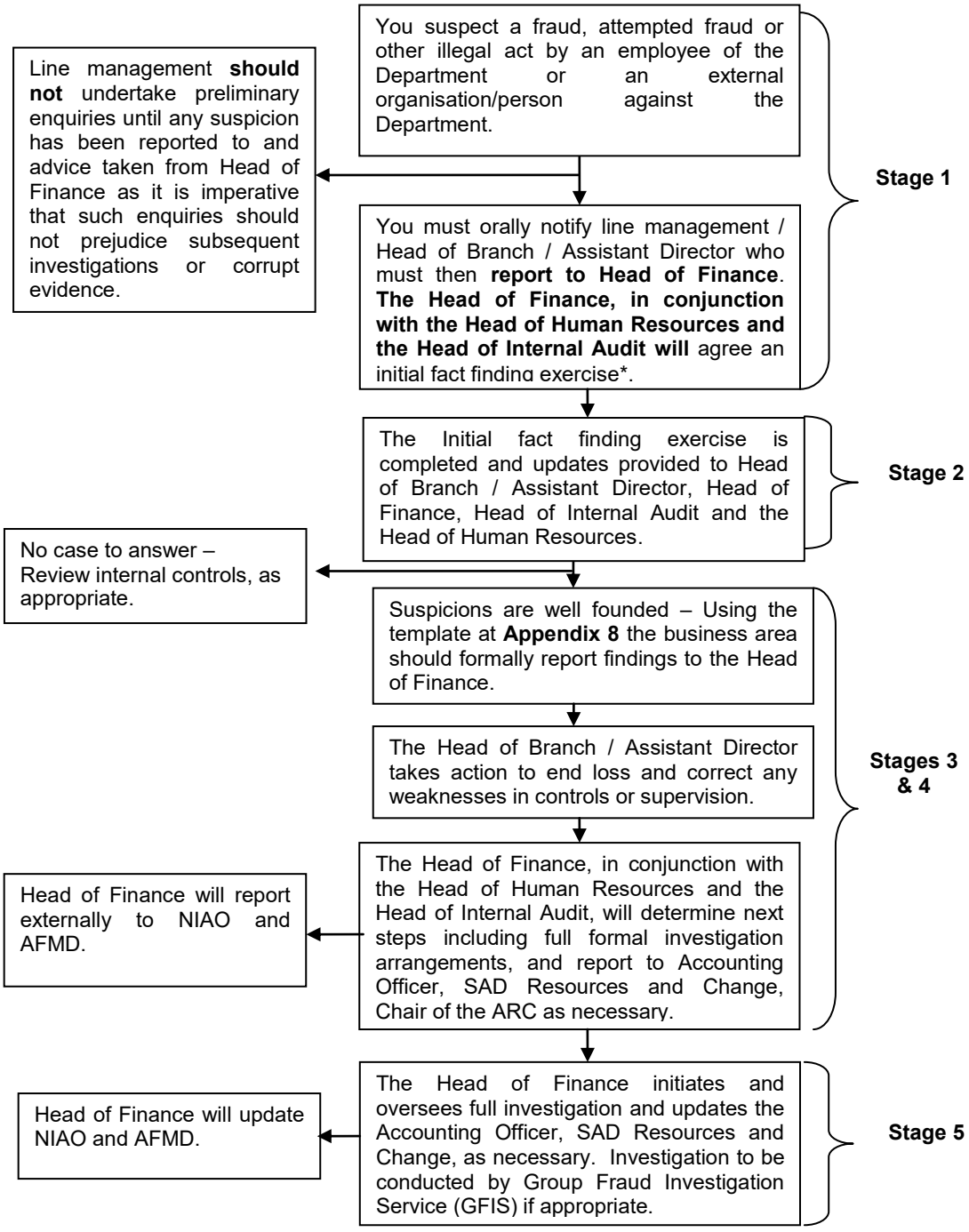
- A similar duty of care exists towards members of staff under investigation, who should be advised of the investigation process, expected timescales and the eventual outcome;
- The Annual Fraud Return will provide a composite account of the Department's fraud cases. Consideration should be given to informing other public sector organisations, e.g. other Government departments, NIAO, grant paying organisations;
- At the appropriate time, inform the PPS Fraud Working Group and the NICS Fraud Forum of outcomes and lessons learned; and
- A lessons-learned document should be circulated throughout the Department, if appropriate.

CONCLUSION

46. Any queries in connection with this **Fraud Response Plan** should be made to the Head of Finance.

47. Current contact details for officers referred to above are provided in **Appendix 5**.

Reporting fraud / suspected fraud



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

ANTI-FRAUD POLICY AND FRAUD RESPONSE PLAN APPENDICIES

Appendix 1 - Indicators of Fraud[2]

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.

[2] Managing the Risk of Fraud (NI) – December 2011, DFPNI, Accountability and Financial Management Division

- 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[3]

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).

[3] Managing the Risk of Fraud (NI) – December 2011, DFPNI, Accountability and Financial Management Division

How fraud could be Perpetrated	Examples of controls
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 authorising 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. • Ensure that countersigning officers pass approved claim forms direct to the finance team. • 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.

How fraud could be Perpetrated	Examples of controls
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	• 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[4]

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.

[4] Managing the Risk of Fraud (NI) – December 2011, DFPNI, Accountability and Financial Management Division

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 - PPS Whistleblowing Policy

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 none of your business or that it is only a suspicion. You may have felt that raising the matter would be disloyal to colleagues, managers or to PPS. 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. PPS has put in place 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 Whistleblowing 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 Whistleblowing arrangements you will help us to achieve this.

A copy of the PPS's Whistleblowing Policy is available on the Department's website/intranet.

Appendix 5 - Contact Details

Name	Designation	Telephone Number
	Head of Finance	
	Head of Human Resources (HR)	
	Head of Internal Audit DoJ (representing PPS)	

Appendix 6 – Guidance on Performing an assessment of Fraud Risks

The PPS risk management process includes a number of steps, as follows:

- Identification of risk;
- Assignment of ownership;
- Prioritisation of risks;
- Risk Responses;
- Assurance; and
- Embedding and review.

Identification of Risk

Identify the key fraud risks facing your business area. Examples might include:

- Fraudulent court witness 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.

Identification and assessment of risks is viewed as a management function, to be considered at all management levels throughout the PPS.

Any statement of risk should encompass the cause of the impact and the impact to the objective (cause and consequence). In identifying risks, managers should not just consider threats to the achievement of their objectives but also consider opportunities for improved performance and enhanced capacity.

Whilst the assessment of risk is largely judgmental, it is necessary to adopt a systematic approach for the identification of risk.

Assignment of Ownership

The Director has overall responsibility for the PPS risk management framework. However in order for risk management to be effective it is essential that responsibility for individual risks is delegated to the appropriate level. Therefore all identified risks will have an 'owner', so that responsibility and authority for implementing action plans is clearly understood.

Within the PPS ownership of corporate risks will usually be assigned at Grade 5 level or above. Although the owner of the risk may not always be the person tasked with the assessment or management of the risk, they are responsible for ensuring the risk framework is applied.

Rating of Risks

A key element in any risk management framework is that it should allow managers to identify the areas of risk in which action needs to be taken and their relative priority.

There is a degree of risk in all of the Service's activities and its ability to take positive action about some risks may be limited or the cost of taking that action may be disproportionate to the potential benefit gained. Control costs money and it is important that any potential loss associated with a risk materialising should be weighted against the cost of controlling it. Each risk is therefore graded using rankings on the likelihood of the risk occurring and the impact it would make if it did occur.

Risks are quantified on a scale of 1 to 4 for both likelihood of occurrence and degree of impact. In order to ensure consistency of approach, a simple 'traffic light' system is used which categorises risk priorities as 'high', 'medium', 'moderate' or 'low'. In line with accepted practice, this will be based on an assessment of the likelihood that an event will occur and its potential impact on the organisation, as follows:

(a) Likelihood x (b) Impact = Risk Priority

(a) Likelihood

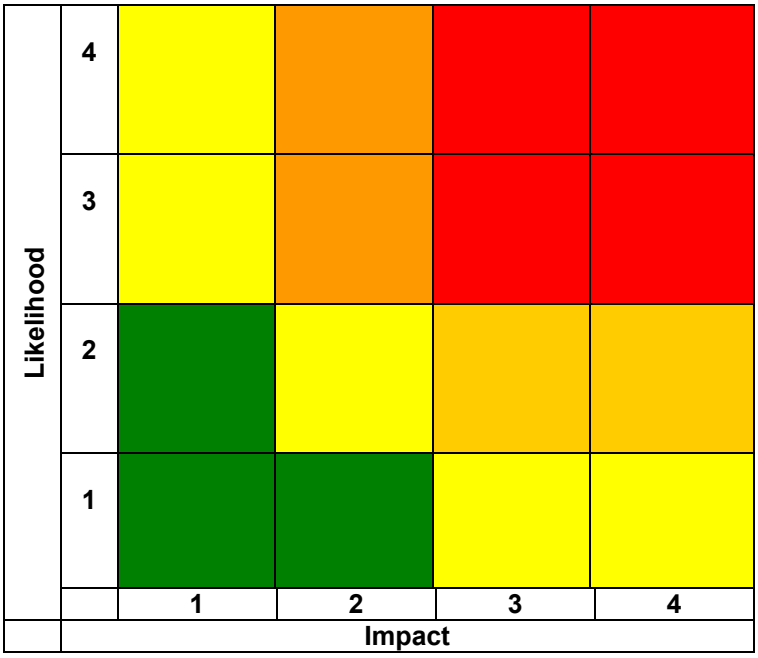
Score	Probability	Description
1	0-25%	Unlikely to occur
2	26-50%	Fairly likely to occur
3	51-75%	More likely than not to occur
4	75%+	Very likely to occur / will occur

(b) Impact

Score	Rating	Description
1	Very Low	Minimal loss, delay, inconvenience or interruption
2	Low	Minor loss, delay, inconvenience or interruption Short to medium term effect
3	Medium	Significant waste of time and resources Impact on operational efficiency, output and quality Medium term effect which may be difficult or expensive to recover
4	High	Major impact on costs and objectives. Serious impact on output / quality and reputation. Medium to long-term effect which may be difficult or expensive to recover

A simple 4 x 4 matrix will be used to prioritise risks according to priority (see below).

PPS Risk Assessment Matrix



Key:

High	The consequences of the risk materialising would be severe and possibly disastrous. Some immediate action is required plus the development of a comprehensive action plan. Red risks require immediate action. 'Showstopper' risks are those that would: • Stop you from meeting your objectives or targets; • Be likely to have major impact on your processes; • Cause severe damage to corporate reputation or public embarrassment.
Medium	Consequences of risk not severe and can be managed via contingency plans. Action plans developed later and budget bids mobilised. Status of risk should be monitored regularly. Amber risks need to be monitored and managed down to yellow / green. Potential risks are those that could: • Prevent you from meeting certain objectives/targets but do not endanger others; • Inconvenience the Department.
Moderate	Consequences of risk remain relatively unimportant to business. However closer monitoring is required. The Service should consider what contingencies (at minimal additional cost) could be put in place to prevent negative outcomes.
Low	Consequences of risk relatively unimportant to business. Status of risk should be reviewed periodically. *Green risks do not require action.* Minor risks are those that have minor impact but do not affect a successful outcome.

Risk Responses

Once a risk has been identified consideration must be given to the appropriate response. Responses to risk can be divided into four categories:

- Transfer;
- Tolerate;
- Treat (Mitigate); or
- Terminate.

Please refer to the PPS Policy & Framework for Risk Management for more details of these categories.

In many cases PPS risks will fall into the *'Mitigate'* category. Where this is the case, actions will be identified and put in place to manage these risks and contain them to as low a level as is reasonably practical (i.e. adopt a proportionate response).

Assurance

The Department obtains assurance on its risk management process through regular monitoring and reporting (via the Management Board, Senior Management Group and relevant project groups), as well as from the Quarterly Assurance Statements, the Audit and Risk Committee and periodic review by Internal Audit.

Embed and Review

The Service integrates risk management within all aspects of the business planning process. Relevant induction / awareness training sessions are also provided to all managers and staff.

Appendix 7 – Best Practice for Reporting Suspicions of Fraud and Irregularity

If staff become aware of a suspected fraud or irregularity, they should write down their concerns immediately, making a note of all relevant details, such as what was said in phone or other conversations, the date, the time and the names of anyone involved. It may be necessary to handover any notes and/or evidence you have gathered to the appropriate investigator.

STAFF MUST NOT DO ANY OF THE FOLLOWING:

- Contact the suspected perpetrator in an effort to determine the facts;
- Discuss the case facts, suspicions, or allegations with anyone outside the Department;
- Discuss the case with anyone within the department other than the people detailed in the **Anti-Fraud Policy and Fraud Response Plan**;
- Attempt to personally conduct investigations or interviews to question anyone.

Action by Managers

If line management have reason to suspect fraud or corruption in the work area, they should:

- Listen to the concerns of their staff and treat every report received seriously and sensitively;
- Make sure that all staff concerns are given a fair hearing. Line Management should also reassure staff that they will not suffer because they have told you of the suspicions;
- Get as much information as possible from the member of staff, including any notes and any evidence they have that may support the allegation. Do not interfere with any evidence and make sure it is kept in a safe place;
- Do not try to carry out an investigation yourself; this may damage any criminal enquiry. Seek advice from Head of Finance before taking any action; and
- **Report the matter immediately to Line Management / Head of Business / Assistant Director who will report to the Head of Finance.**

Appendix 8 – Formal Notification of Frauds

From: [Business Area]

To: Head of Finance

1.	Departmental fraud reference number (unique identifier)	*e.g. 2016/17 – PPS 1.(To be completed by the Head of Finance)*
2.	Department	Public Prosecution Service
3.	Name of body (eg specific Board, Trust, NDPB, Agency etc)	N/A
4.	Specific location of fraud (eg 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?	*Actual, Suspected or Attempted*
7.	Type of fraud?	*State as per options listed in notes 1*
8.	What was the cause of the fraud?	*State as per options listed in notes 2*
9.	Brief outline of case	
10.	Amount of lost or estimated value?	
11.	How was the fraud discovered?	*State as per options listed in notes 3*
12.	Who perpetrated the fraud?	*State as per options listed in notes 4*
13.	Has PSNI been notified?	Yes / No
14.	Any other action taken so far?	*State as per options listed in notes 5*
15.	Please give contact details for this fraud in case follow-up is required	Name: Telephone: Email:

Notes

1. Types of fraud

- Grant related
- Theft of assets (please state type of asset eg cash, laptop, oil, tools, camera)
- Payment process related
- Income related
- Pay or pay related allowances
- Travel and subsistence
- Pension fraud
- Contractor fraud
- Procurement fraud
- False representation
- Failure to disclose information
- Abuse of position
- Other (please specify)

2. Causes of fraud

- Absence of proper controls
- Failure to observe existing controls
- Opportunistic
- Unknown

3. Means of discovery of fraud

- Normal operation of control procedures
- Whistleblowing (internal or external)
- Internal Audit

- External
- Computer analysis/National Fraud Initiative
- Other means (please specify)

4. Perpetrators of Fraud

- Internal staff member
- Contractor
- Funded body/grant applicant
- Other third party (please specify)
- Collusion between internal and external parties
- Too early to determine
- Unknown

5. Other actions taken

- Controls improved
- Control improvements being considered
- Too early to determine
- No action possible
- Disciplinary action
- Prosecution

Appendix 9 – Summary of Good Practice Guidance issued by the NICS Fraud Forum: when carrying out a Fraud Investigation involving Purchasing and Payment of Invoices[5]

This guidance was developed by the Fraud Forum following one department's review of a fraud investigation it had undertaken.

The issues listed below are not designed to provide comprehensive guidance to those undertaking fraud investigations but are designed to be of use to investigators who may find themselves undertaking a similar type of investigation and who may benefit from knowing about the experiences of others.

The general lessons learned were:

- Where fraud occurs or is suspected prompt and vigorous investigations should be carried out by officers independent of the work areas under investigation.
- The investigation should be carried out by fully trained and experienced investigators with a working knowledge of interviewing suspects and collecting evidence in accordance with the provisions of the Police and Criminal Evidence (Northern Ireland) Order 1989.
- The PSNI should be informed and advice sought at the earliest possible juncture.
- All aspects of the suspected fraudster's work should be investigated, not just the area where the fraud was discovered.
- The investigation will obviously 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 computer files and record of amendments relevant to the case should be retained and not disposed of regardless of the normal routine procedures for disposal.
- Control weaknesses discovered in procedures during the investigation should be strengthened immediately.

[5] Managing the Risk of Fraud (NI) – December 2011, DFPNI, Accountability and Financial Management Division

Useful checks to apply

- Departmental staff, including finance, internal audit and those responsible for fraud investigations should consider the merits of adding the checks, listed below to their control procedures and investigation/audit programmes. Consideration should also be given to building in some of these checks when systems are under development. Some of the checks listed may come under the provisions of the Data Protection legislation and so advice from the Information Commissioner's Office may need to be sought.

Master File Standing Supplier Data

1. Comparison of the master file standing supplier data against staff personal bank account data recorded on the payroll system.
2. Historical amendments to the master file standing data should be checked to identify any temporary changes to the bank account details or the creation of temporary fictitious suppliers.
3. Comparison between the bank account details held on the master file standing supplier data and the bank accounts into which monies were actually paid.
4. Reasonableness checks on the master file standing supplier data to establish the location of the bank into which the monies were paid and comparison with the address of the supplier. Bank locations are identified by the sort codes.

Purchase Ledger Transactions

5. Test the purchase ledger transactions for multiple use of the same order number against invoices from different suppliers.
6. Test the purchase ledger transactions for different suppliers with the same bank account number.
7. Test the purchase ledger transactions for invoices posted without a purchase order number.

Documentation

8. Check invoice files for photocopied invoices and purchase orders and investigate further.

9. Check for instances where the purchase orders were raised after the invoices had been received.
10. Check for payments made on supplier statements rather than on invoices.
11. Review purchase orders and goods received notes (GRN's) to identify those transactions that have been ordered and the goods evidenced as received by the same person.

Paid Cheques

12. Examine the paid cheques to identify the bank, the account number and the sort code into which the cheque was deposited. The purpose being to establish whether payments to the same supplier had been lodged into different bank accounts. Compare with details held on the standing data.
13. Examine paid cheques for endorsements to determine whether cheques were endorsed to a third party and lodged into an account other than the supplier.

Cash Book

14. Investigate outstanding lodgements and outstanding cheques recorded on the bank reconciliations to ensure that they are legitimate.