MANAGING THE RISK OF FRAUD

A GUIDE FOR MANAGERS

HM TREASURY

Assurance,
Control and Risk

May 2003

HM TREASURY

MANAGING THE RISK OF FRAUD

A Guide for Managers

May 2003

HM Treasury contacts

Comments on the coverage or presentation of this report should be sent to:

Richard Fennelly
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

E-mail: richard.fennelly@hm-treasury.x.gsi.gov.uk

For enquiries about the Treasury and its work, contact:

Treasury Public Enquiry Unit:

Tel: 020 7270 4558

Fax: 020 7270 4574

E-mail: public.enquiries@hm-treasury.gov.uk

This document can be accessed from the Treasury's Internet site at:
www.hm-treasury.gov.uk

CONTENTS

APPENDICES:

1. Introduction

Departmental responsibilities in relation to the management of fraud risk are set out in Chapter 5 of Government Accounting 2000. The purpose of this booklet is to show how the principles of sound risk management, governance and control apply to fraud and other irregular activities that might lead to fraud. The booklet:

- Concentrates on the management of fraud risks; it does not attempt to provide a complete approach to risk management[1].
- Provides guidance on options for controlling identified fraud risk to acceptable levels of exposure.

Sections 2 – 5 provide a summary of the management of fraud risk. **Section 6** provides managers, at all levels, with more detail about managing their individual responsibilities in relation to fraud risk.

This publication updates an earlier version that was issued in November 1997.

2. What is Fraud?

There is currently no precise legal definition of fraud.

For the purposes of reporting fraud to the Treasury the following crimes fall within the context of the Fraud Report:

Theft

Dishonestly appropriating the property of another with the intention of permanently depriving them of it (Theft Act 1968). This may include the removal or misuse of funds, assets or cash.

False Accounting

Dishonestly destroying, defacing, concealing or falsifying any account, record or document required for any accounting purpose, with a view to personal gain or gain for another, or with intent to cause loss to another or furnishing information which is or may be misleading, false or deceptive (Theft Act 1968).

Bribery and Corruption

The offering, giving, soliciting or acceptance of an inducement or reward that may influence the actions taken by the authority, its members or officers (Prevention of Corrupt Practices Acts 1889 and 1916).

Deception

Obtaining property or pecuniary advantage by deception (sections 15 and 16 of the Theft Act 1968) and obtaining services or evading liability by deception (sections 1 and 2 of the Theft Act 1978).

[1] For information on the principles of risk management used in the guidance see 'Management of Risk - A Strategic Overview' www.hm-treasury.gov.uk

Collusion

The term "collusion" in the context of reporting fraud to the Treasury is used to cover any case in which someone incites, instigates, aids and abets, conspires or attempts to commit any of the crimes listed above.

3. How fraud occurs

Four basic elements are necessary for a fraud to occur:

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

Managers must ensure that the opportunities for fraud are minimised. While some people would never contemplate perpetrating a fraud, others may if they thought they could get away with it. A high chance of being caught will deter. 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 (see **Appendix 7** for more information).

4. Fraud Risk

Fraud is just one of many risks an organisation faces. However, the deliberate nature of fraud can make it difficult to detect and deter.

Risk, in the context of managing fraud risk, is the vulnerability or exposure an organisation has towards fraud and irregularity. It combines the probability of fraud occurring and the corresponding impact measured in monetary terms. Preventive controls and the creation of the right type of corporate culture will tend to reduce the likelihood of fraud occurring while detective controls and effective contingency planning can reduce the size of any losses.

5. Fraud Risk Management – an Overview

Everybody in an organisation contributes to the management of fraud risk. This starts at the top where senior management set the tone of the organisation and promote an anti-fraud culture throughout the organisation. Operational staff design and implement and operate the control actions required to minimise risk. The personnel function ensures that the right staff are recruited. Accommodation services ensure physical security and IT services promote computer and data security. The role of internal audit is to deliver an opinion to the Accounting Officer on the whole of an organisation's risk management, control and governance. In relation to fraud this will include the examination of the adequacy ofarrangements for managing the risk of fraud and ensuring that the organisation actively promotes an anti-fraud culture.

The Accounting Officer is responsible for maintaining a sound system of internal control that supports the achievement of departmental policies, aims and objectives, whilst safeguarding public funds and departmental assets in accordance with Government Accounting. The internal control system should be designed to respond to and manage the risks which departments face in the achievement of their policies, aims and objectives. Managing fraud risk should be seen in the context of the management of this wider range of risks. The responsibility for the overall management of anti-fraud activities should be allocated to an appropriate senior officer e.g. the Principal Finance Officer [see **Appendix 1**].

A clear statement of commitment to ethical behaviour throughout the organisation should help to ensure that staff know that they are expected to follow the rules without circumventing controls and that they should avoid or declare any conflicts of interest. The seven principles of public life set out in the Nolan Committee's report on Standards in Public Life are relevant here (i.e. selflessness, integrity, objectivity, accountability, openness, honesty and leadership - see **Appendix 2**).

Senior Management should try to create the conditions in which staff have neither the motivation nor the opportunity to commit fraud. The maintenance of good staff morale may help to minimise the likelihood of an employee causing harm to the organisation through fraud.

Under the right conditions staff are themselves an excellent deterrent against fraud. There should be avenues for reporting suspicions of fraud. Staff should be encouraged to report suspicions of fraud either to their line managers, to internal audit or to a hotline set up for this purpose.

The organisation's approach to fraud, which contributes to an anti-fraud culture, should be communicated throughout the organisation, including contractors and third parties delivering services on behalf of the organisation.

Two key documents, used in promoting an anti-fraud culture are the **Fraud Policy Statement** and **Fraud Response Plan**; these are described in more detail in **Appendices 3 and 4**. Such documents are considered to be the **minimum requirement** for any organisation in managing the risk of fraud. Anti-fraud policies should make it absolutely clear "to all those who seek to defraud the government that such action is unacceptable and will not be tolerated" (Government Accounting 2000, Chapter 5, paragraph 5.1.1). Most people accept that this does not mean that fraud can be wiped out totally or that it is cost effective to prosecute every suspected case through the courts. Changing people's attitudes to the social acceptability of fraud can take several forms such as statements in departmental policies, warnings on official forms, publicity campaigns and policy statements on websites.

In addition departments should undertake a systematic assessment of fraud risk. The level and depth of this assessment will be determined by the vulnerability or exposure an organisation feels it has in relation to fraud and irregularity. Fraud risk assessment is described in more detail in **Section 6.**

Further Guidance

Some large departments have an inherent risk of fraud (e.g. welfare benefit abuse, tax evasion, prescription fraud). Whilst the general principles in this guidance apply to all departments, it should be recognised that those departments with a high risk of fraud will have developed targets, measures and procedures to reduce the level of fraud risk and this can be an additional source of guidance and good practice for others in developing their own anti-fraud strategies.

Fraud seminars, held regularly by the Treasury, attempt to bring to the attention of anti-fraud practitioners examples of good practice developed by others in the public sector.

Additionally, in order to promote cooperation and joint working between different fraud units in other government departments and local authorities, a number of anti-fraud networks have been developed (e.g. DfES Fraud Response Liaison Group, CIPFA's Better Governance Forum Advisory Panel[2]).

6. Managing the Risk of Fraud – a risk based approach

A risk-based approach enables organisations to target their resources, both for improving controls and for pro-active detection, at problem areas. Developments in corporate governance, including the requirement for statements on internal control[3], create the atmosphere in which fraud can be considered as a set of risks to be managed alongside other business risks. Managing the risk of fraud should be embedded in the entirety of an organisation's risk, control and governance procedures.

In broad terms managing the risk of fraud involves:

- Assessing the organisation's overall vulnerability to fraud [see **6.1**];
- Identifying the areas most vulnerable to the risk of fraud [see **6.2**];
- Assigning ownership [see **6.3**];
- Evaluating the scale of fraud risk [see **6.4**];
- Responding to the risk of fraud [see **6.5**]; and
- Measuring the effectiveness of the fraud-risk strategy [see **6.6**].

6.1 Assessing the Organisation's Overall Vulnerability to Fraud

Vulnerability to fraud can be assessed at different levels in an organization. A quick assessment of the overall level of risk an organisation is exposed to is often a good starting point and may highlight particular vulnerabilities where some action needs to be taken immediately rather than wait for the results of a more in-depth risk assessment to be completed. The checklist in **Figure 1** provides a list of questions that might be used to gain an overall assessment of an organisation's fraud risk, and introduces some of the elements necessary for managing those risks.

In organisations where the risk of fraud is known to be high, a separate specific fraud risk assessment and evaluation may be appropriate [see **6.2** and **6.4**]. Where the risk of fraud is considered to be low a specific fraud risk assessment may not be necessary, any risks being considered instead as part of the organisation's overall risk assessment as set out in the "Orange Book"[4]. However it will still be necessary for those organisations to develop an anti-fraud culture as outlined in **6.5.1.**

A fraud risk assessment should additionally be carried out during the development of any new policies, activities or operations to ascertain whether any new risks arise that need to be managed. The risk assessment should also be reviewed and re-assessed whenever a change in policy occurs or when changes are made to the way in which a policy is to be implemented.

[2] www.ipf.co.uk/Governance/
[3] DAO [GEN] 13/00
[4] For more information on risk see "Management of Risk - a Strategic Overview" (the Orange Book")

6.2 Identifying the Areas Most Vulnerable to Fraud

The overview of fraud [**6.1**] will show the scale and nature of fraud faced by the organisation and the relative risks between different types of fraud. This will determine whether there is a need to perform a more detailed assessment of those risks to provide a guide as to where the department should focus its efforts in improving control.

This more detailed assessment of fraud risk will result in an "exposure profile" or fraud risk framework that identifies the areas in which an organisation may face fraud threats and the types of threat it may face. It will not be cost effective to cover every possible threat situation therefore the likely occurrence of potential fraud, and the impact on key organisational objectives must be assessed. The steps in this stage include[5]:

- Identifying the processes or activities at risk of fraud (**Figure 2**). These can be identified using a number of techniques including:
  - o Commissioning a risk review;
  - o Undertaking risk self-assessment through: facilitated workshops and interviews; brainstorming; questionnaires; process mapping; and discussions with peers.
  - o Benchmarking – comparisons with other organisations.
  - o Assessing and ranking the nature and extent of vulnerability in each area [**Figure 3**].
  - o Identifying the particular forms of fraud threat to each area [**Figure 4**].

6.3 Assigning Ownership

It will be necessary to allocate responsibility for the overall management of fraud risk and for the management of anti-fraud activities.

All those responsible for managing resources should be aware of the associated fraud risks. The ultimate responsibility and accountability for fraud risk rests with the Accounting Officer although specific responsibility for managing the risk of fraud may be allocated to an appropriate senior officer such as the PFO. Where appropriate, the responsible officer should liaise with the Risk Management Committee and/or Audit Committee in order to ensure that there is consistency in the scoring of fraud risk and in action taken to manage it. However, some fraud risks will require day-to-day management and it will be important to assign responsibility for managing specific risks, once identified, at appropriate levels in the organisation. Establishing accountability and responsibility for specific fraud risks is necessary to:

- Encourage a culture of fraud risk awareness throughout the organisation;
- Ensure fraud risk remains well controlled; and
- Create a framework for the provision of reporting on the management of fraud risk to senior management.

Appendix 1 covers responsibilities for fraud risk ownership in more detail.

[5]Source: the Audit Office of New South Wales (see http://www.audit.nsw.gov.au under "Reports, Guides and Publications" and "Guides to Better Practice")

Checklist for assessing overall fraud risk

- Does the organisation view fraud within the context of wider risks (e.g. the risk of errors and irregularities)?
- Is there a definition of the processes or activities open to fraud? It is fundamental to fraud risk assessment to know the scope of the problem the organisation is managing.
- If the risk of fraud is considered to be high is there a fraud risk assessment including a comprehensive risk log? The fraud risk assessment should include, as a minimum, a basic register or log that identifies the risks. It should include a separate assessment of both the impact and the likelihood of each risk and should be a living document that is continuously updated to reflect changing circumstances.
- Does the organisation have effective recruitment procedures to reduce the risk of employing potential fraudsters? Confirm that employee details and references are thoroughly checked.
- How does the organisation demonstrate zero tolerance to fraud? Government bodies should have a policy demonstrating to all those that might seek to defraud the Government that such action is not acceptable and will not be tolerated. This can take many forms such as wording on claim forms and declarations, advertising campaigns, statements on websites, and publicity about sanctions including prosecutions. All staff and external contractors should be aware of the organisation's attitude to fraud and their consequences.
- Is there a clear statement of commitment to ethical business behaviour throughout the organisation to help ensure that staff know that they are expected to follow the rules without circumventing controls and that they should avoid or declare any conflicts of interest?
- Does the organisation have a fraud policy statement to communicate the organisation's approach to fraud? Such a statement may include some or all of the following areas:
  - Allocation of responsibilities for the overall management of fraud;
  - The procedures which staff should follow if fraud is discovered;
  - Guidance on training for the prevention and detection of fraud;
  - Reference to response plans that have been devised to deal with and minimise the damage caused by fraudulent attack.
- Does the organisation have a fraud response plan? It is important that managers know what to do in the event of fraud so that they can act without delay. An effective fraud response plan should be closely tailored to each organisation's circumstances and should reflect the likely nature and scale of losses. A fraud response plan should cover:
  - To whom the fraud or suspicion of fraud should be reported in the first instance (e.g. senior managers, personnel or internal audit);
  - How the organisation should investigate fraud;
  - How to secure evidence in a legally admissible form;
  - When and how to contact the police;
  - How to initiate recovery action;
  - Who else to contact for advice (e.g. insurers, regulatory bodies, legal advisers, parent department, press office);
  - How to disseminate the lessons learned from fraud cases.
- Does the organisation have an effective fraud awareness programme?
- Does the organisation have clear reporting channels for reporting suspicions of fraud that offer protection to those reporting fraud? Suitable avenues can include line management, senior management, a specialist fraud team or internal audit. Organisations can also establish fraud hotlines so that staff can report suspicions of fraud confidentially. It is important that all cases of reported fraud or suspicions of fraud are acted upon.
- Does the organisation have an effective framework for reporting details of fraud and thefts to the Treasury to meet the requirements of Government Accounting 2000, chapter 5?

Figure 1

Identifying the Processes or Activities at Risk to Fraud

The starting point is to identify the organisation's major activity areas in terms of:

- Product and service outputs and deliverables;
- Operational areas and locations;
- Revenue generation;
- Revenue collection;
- Expenditure;
- Suppliers and inputs;
- Asset utilisation, acquisition and disposal;
- Customer/client records and support.

Figure 2

Assessing and ranking the nature and extent of vulnerability in each area

A rating should be given to each of the areas identified in the previous step in terms of its potential vulnerability to both internal and external fraud. All areas should be ranked by their vulnerability factor and listed from the highest down to the lowest. Some common criteria/factors used to make judgements about vulnerability include:

- Materiality;
- Economic indicators;
- Fraud history;
- Last time the activity/function was reviewed;
- Concerns of management;
- Staff attitudes and values;
- Management attitudes and values;
- Quality of management;
- Internal control history for the area;
- Extent of effective reporting mechanisms;
- Internal and external audit risk assessment ratings for the area;
- Degree of operational complexity;
- Overall size, scope and value of activities;
- Impact of technology.

Figure 3

Identifying the Particular Forms of Fraud Threat to Each Area

Each area can be assessed in terms of particular forms of threat such as:

- Theft;
- Misappropriation of funds or assets;
- Fraudulent administration of contracts;
- Falsification of source records for improper advantage.

Figure 4

6.4 Evaluating the Scale of Fraud Risk

In deciding how to handle the fraud risks identified in the exposure profile it is important to evaluate their significance. Risk evaluation and assessment will inform decisions about the areas of risk where action needs to be taken, and the relative priority of those risks. **Figure 5** illustrates just one approach to this.

An analysis of threats against compensating factors such as internal controls is a key part of this task. This phase of the risk assessment seeks to determine the extent to which existing internal controls are sufficient to counter the fraud threats that have been identified [see **6.5.2**]

Evaluating the scale of fraud risks

Once risks have been identified, an assessment of the possible impact and corresponding likelihood of occurrence should be made using consistent parameters that will enable the development of a prioritised risk analysis. Management should agree on the most appropriate definition and number of categories to be used when assessing both the likelihood and impact of each risk. The assessment of the impact of the risk should not simply take account of the financial impact but should also consider the organisation's reputation, and recognise the potential political and commercial sensitivities involved. The analysis should be either qualitative or quantitative, and should be consistent to allow comparisons. The qualitative approach usually involves grading risks in high, medium or low categories[6].

Figure 5

[6]Source: CIMA: 'Fraud Risk Management - a guide to good practice' (http://www.cimaglobal.com/downloads/tec_fraud_risk_mngmnt.pdf)

6.5 Responding to the Risk of Fraud

Once the risks have been evaluated and prioritised consideration can be given to identifying appropriate responses. Responding to the risk of fraud involves compiling anti-fraud control policies and fraud response plans. Additionally it also involves putting in place effective accounting and operational controls and the maintenance of an ethical climate that encourages staff at all levels to actively participate in protecting public money and property.

Responses to fraud risk include:

- Developing and promoting an anti-fraud culture [**6.5.1**].
- Allocating responsibilities for the overall management of fraud risk and for the management of specific fraud risks [**6.3**].
- Establishing cost effective internal controls to detect and deter fraud that are commensurate with the identified risk [**6.5.2**].
- Establishing anti-fraud related PSA/SDA targets where appropriate [**6.5.3**].
- Developing the right skills and expertise required to manage the risk of fraud effectively and to respond effectively to fraud when it occurs [**6.5.4**].
- Responding effectively to fraud when it occurs [**6.5.5**].
- Establishing appropriate avenues for reporting fraud [**6.5.6**].
- Monitoring the implementation of specific actions determined by management to reduce the risk of fraud [**6.5.7**].
- Continuously monitoring the risk environment [**6.5.8**].

6.5.1 Developing and promoting an anti-fraud culture

These areas are covered in more detail in **Appendix 2**.

Creating an anti-fraud culture involves:

- Having a clear statement of ethical values;
- Establishing a clear anti-fraud policy (**Appendix 3**) and fraud response plan (**Appendix 4**);
- Promoting staff awareness of fraud;
- Recruiting honest staff (checking references etc); and
- Maintaining good staff morale.

6.5.2 Establishing cost effective internal controls that are commensurate with the identified risk

There are a range of controls (e.g. physical checks, reconciliation, supervisory checks, segregation and rotation of duties, and clear roles and responsibilities) that address risk, including that of fraud. Departmental managers should consider which controls are most appropriate in their particular circumstances. In designing control, it is important that the control put in place is proportional to the identified risk. 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.

Internal control can be classified in four ways:

- **Detective controls**: those established to spot errors, omissions and fraud after the events have taken place. See **Appendix 5** for more information about detecting fraud. **Appendix 6** is a list of useful Fraud Indicators.
- **Directive controls**: those designed to ensure that a particular outcome is achieved. An example of this type of control is that staff be required to put the fraud response plan into action immediately a fraud is suspected or discovered;
- **Preventive controls**: those designed to limit the possibility of an undesirable outcome (e.g. a fraud) being realised. These are covered in **Appendix 7**.
- **Corrective controls**: those designed to correct undesirable outcomes that have been realised.

For examples of internal controls in specific areas see **Appendix 8**.

6.5.3 Establishing anti-fraud related PSA/SDA targets

The requirement to cover fraud in SDAs does not preclude the possibility of fraud targets in those PSAs where anti-fraud work may be of major political significance. Fraud is usually used to describe depriving someone of something by deceit. Errors in payments and other irregularities are extremely costly too, and should be a cause for concern and managerial corrective action. Rather than focusing on actual or possible crimes, it is therefore often sensible to look at irregularities more broadly - if high rates of error indicate some systemic or managerial problems in an area, it can also be a good signal of where anti-fraud attention should be targeted. Government has to consider two different types of fraud - internal and external. The most appropriate measures will vary from department to department, and targets are only likely to be appropriate where there is a significant problem. Targeting fraud and error is also not simple.

Whilst the obvious targets may be detection (and even recovery) rates, it is also vital to encourage fraud and error prevention, as it is the overall reduction in the volume of irregularity that is at issue. Targets focused on detection alone, without also monitoring prevention, can lead to perverse results, actually encouraging prevention slackness. [Source: sr2002 guidance[7]]

Work done by those departments with an inherent risk of fraud (e.g. DWP, Inland Revenue, Customs and Excise, NHS) can be a useful source of guidance about setting targets and measures to be used to reduce the level of fraud risk faced. Useful sources of information include:

[7] http://www.hm-treasury.gsi.gov.uk/psd/sr2002/sr2002_final_guidance/sr2002guidance3targets.htm#Introduction

- NAO Report – Tackling Benefit Fraud (HC393 Session 2002-03: 13 February 2003);
- NAO Report – Fraud Against the Inland Revenue (HC 429 Session 2002-03: 28 February 2003);
- NHS: Directorate of Counter Fraud Services (http://www.doh.gov.uk/dcfs/index.htm).

6.5.4 Developing the right skills and expertise

This can be achieved by:

- Developing competency levels for both specialist anti-fraud personnel and more general operational staff, and
- Identifying a range of training courses/development events designed to enable staff to meet those competency levels. These can either be developed "in-house" or procured, and can include:
  - o events on general subjects e.g. fraud identification, preventing fraud, IT crime, or
  - o technical and specialist courses for key staff (e.g. managing a fraud incident, investigating a fraud, interviewing).

6.5.5 Responding effectively to fraud when it occurs

Depending on the significance of the fraud, the fraud investigation process involves some or all of the following:

- Ensuring that the actions to take if fraud is discovered are clearly described in the organisation's Fraud Response Plan.
- Senior management providing the direction for any fraud investigation.
- Establishing clear terms of reference for the investigation.
- Appointing a Fraud Investigation Officer (FIO) to take charge of the investigation (usually a senior manager).
- Setting up a mechanism to report on progress of the investigation to appropriate senior levels of management.
- Controlling the investigation through procedures set out in the Fraud Response Plan.
- The overall investigation process involves:
  - o Maintaining confidentiality;
  - o Recovering assets;
  - o Forensic investigations and protection of evidence;
  - o Interviewing witnesses and dealing with employees under suspicion;

- Controlling police involvement;
- Managing civil proceedings;
- Liaising with experts and regulators;
- Preparing media statements; and
- Reporting progress and findings to senior management.

- Ensuring that effective controls are in place to preserve all forms of evidence. This is a key factor if the fraudster is to be prosecuted successfully as evidence must be legally admissible in court.
- Deciding at an early stage the action to be taken with persons under suspicion and whether suspension or dismissal is necessary. Arrangements for interviewing suspects must be made and if criminal proceedings are initiated the Police must be involved.
- Adhering to a "fair and reasonable" approach in interviews at all times.
- Setting up adequate measures to protect the business throughout the investigation process particularly when issuing statements to the media.
- Initiating a thorough review of all operating procedures in areas affected by the fraud. Comprehensive reports presented to management should set out:
  - Findings;
  - Perceived weaknesses;
  - Lessons learned; and
  - Improvements required to reduce the risk of recurrence.

6.5.6 Establishing appropriate avenues for reporting fraud

There should be avenues for reporting suspicions of fraud. Staff should be encouraged to report suspicions of fraud either to their line mangers, to internal audit or possibly to a hotline set up for the purpose. It is important that staff know where to report their suspicions and that any suspicions of fraud reported in this way are seen to be acted upon by management. Members of the public should also be encouraged to report their suspicions of fraud through advertising campaigns, offering rewards, ensuring that avenues for reporting fraud are widely publicised and assuring whistleblowers that any information received will be treated confidentially.

Of interest in this area is the Public Interest Disclosure Act 1998 which came into force on 2nd July 1999. The Act takes effect as an amendment of the Employment Rights Act 1996 and, as an employment rights measure, provides remedies for workers who are dismissed or subject to detriment for making qualifying disclosures. In protecting workers who make responsible disclosures, it should also help encourage a climate of greater openness and accountability in dealing with wrongdoing within organisations, public and private sector alike. It does this by providing some protection to whistleblowers from unfair dismissal and victimisation.

6.5.7 Monitoring the implementation of specific actions determined by management to reduce the risk of fraud

A system is required to monitor and follow up implementation of specific actions determined by management. A detailed timetable should be established for each item requiring action and regular progress reports produced for senior management review. It is essential to monitor this timetable through the Risk Committee, where an organisation has such a body, through the Audit Committee when there is no separate Risk Committee or for somebody to monitor and report to senior management.

6.5.8 Continuously monitoring the risk environment

The risk environment is constantly changing and priorities of objectives and the consequent importance of risks on the fraud risk profile will shift and change. Risk models have to be regularly revisited and reconsidered in order to have assurance that the fraud risk profile continues to be valid. Control systems should be reviewed at regular intervals and in particular after restructuring, downsizing, changes in business processes, following identification of weaknesses, the introduction of new computer systems, and after an incident of fraud. The risk of fraud should also be considered along with other risks when major new policies are being developed, where a change in policy occurs or where changes are made to the way in which policy is to be implemented.

6.6. Measuring the Effectiveness of the Fraud-risk Strategy

It is essential that assurance about the effectiveness of actions taken to reduce the risk of fraud be obtained. The person assigned responsibility for the management of anti-fraud activities [**see 6.3**] will need to be aware of the many different ways that assurances can be obtained:

- Reporting: "Stewardship Reporting". This is where designated managers report upwards to the Accounting Officer at least annually, through the mechanisms established for risk ownership, assurances on the work they have done to manage risk and operate the appropriate control procedures;
- Where Control Risk Self Assessment is used, the results of exercises and assurances obtained should be reported through the risk owner to the Accounting Officer;
- Internal Audit. The primary role of internal audit is to provide an independent and objective opinion to the Accounting Officer on risk management, control and governance, by measuring and evaluating their effectiveness in achieving the organisation's agreed objectives. Internal audit also provides an independent and objective consultancy service to help line management improve the organisation's risk management, control and governance[8];
- PSA/SDA monitoring systems provide management information which can contribute to the overall assurance;
- The work of other review bodies (e.g. Accounts Inspection Teams, Compliance Review Teams) can also contribute to the overall assurance.

[8]Government Internal Audit Standards [GIAS] - effective from April 2002

In gaining an assurance about the overall effectiveness of the anti-fraud measures established by the organisation it will be necessary for a judgment to be formed based on the various forms of assurance available. Some coordination of the reporting mechanisms will therefore be necessary to facilitate this process.

7. Reporting Fraud to the Treasury

Government Accounting 2000, Chapter 5, requires government departments and their agencies to report details of thefts and fraud within certain categories to HM Treasury annually (e.g. internal frauds, contractor frauds, some other frauds that contain useful lessons for a wider audience). Central government bodies are also required to report details of any novel or unusual frauds to the Treasury as soon as they become aware of them. Treasury will circulate details of cases to other government bodies so that they can be aware of the risks, and can take appropriate measures to reduce the risk of similar frauds being perpetrated against them. Sponsor departments are also required to collect data about fraud committed in their Agencies, NDPBs and other bodies for which they are responsible. Departments should establish suitable information systems for the collection; secure storage and retrieval of data relating to all thefts and fraud perpetrated against them and the bodies for which they are responsible.

Treasury also seeks information concerning the means by which departments develop their anti-fraud strategies. An annual questionnaire is issued to every central government organisation seeking answers to such questions as:

- Does the organisation have an anti-fraud policy?
- Is fraud risk regularly reviewed as part of the organisation's overall assessment of risk?
- Does the organisation have a fraud response plan?
- Does the organisation have a clearly established avenue for "whistleblowers"?

Treasury uses the information collected above to produce an annual Fraud Report that aims to inform departments of the scale and nature of certain categories of fraud, the circumstances in which these frauds occurred, the means by which they were recovered and the action taken against offenders. The information is provided to help departments learn from the experiences of others when reviewing and developing their own systems. The report also aims to increase awareness of fraud risk in specific areas and suggests ways in which the risk can be managed and reduced.

Appendix 1

Responsibilities for Managing the Risk of Fraud - Risk Ownership

Accounting Officers

The Accounting Officer (AO) is personally accountable for his/her organisation and its risk management. A framework of senior level delegation is essential to ensure that the responsibility and authority for implementing control actions is clear. A mechanism for reporting to the AO on risk issues should be established. Managing fraud risks [internal and external fraud risks] is part of the management of all other risks and the same principles apply.

Senior Management

Overall responsibility for Managing the Risk of Fraud should be allocated to an appropriate senior officer, e.g. the Principle Finance Officer. Their specific responsibilities, which can be formally delegated, will depend to some extent with the level of fraud risk the organisation is exposed to but should include some or all of the following:

- Developing a fraud risk profile and undertaking an annual review of the fraud risks associated with each of the key organisational objectives in order to keep the profile current;
- Establishing an effective anti-fraud policy and fraud response plan, commensurate with the level of fraud risk identified in the fraud risk profile;
- Developing appropriate fraud targets – SDA and/or PSA;
- Designing an effective control environment to prevent fraud commensurate with the fraud risk profile;
- Establishing appropriate mechanisms for:
    - reporting fraud risk issues;
    - reporting significant incidents of fraud to the AO;
    - reporting to the Treasury in accordance with GA 2000 Chapter 5; and
    - coordinating assurances about the effectiveness of anti-fraud policies to support the Statement of Internal Control.
- Liaising with the Risk Management Committee and/or Audit Committee as appropriate – where an organisation has a Risk Management Committee it may be appropriate for the reports to go to the AO via that committee. It may also be helpful to ask the Audit Committee to regularly consider fraud risk management issues and significant instances of fraudulent activity;
- Making sure that all staff are aware of the organisation's anti-fraud policy and know what their responsibilities are in relation to combating fraud;
- Developing skill and experience competency frameworks;

- Ensuring that appropriate anti-fraud training and development opportunities are available to appropriate staff in order to meet the defined competency levels;
- Ensuring that vigorous and prompt investigations are carried out if fraud occurs;
- Taking appropriate legal and/or disciplinary action against perpetrators of fraud;
- Taking appropriate action to recover assets;
- Ensuring that appropriate action is taken to minimise the risk of similar frauds occurring in future.

Operational Managers

Outside of any more formal delegation of the above duties, all other levels of management are respon-sible for:

- Implementing and maintaining effective controls to prevent fraud commensurate with the fraud risk profile, and
- Ensuring compliance with anti-fraud policies and fraud response plan.

Individual members of staff

Individual members of staff have an important role to play in combating fraud. Their responsibilities include:

- Acting with propriety in the use of official resources and in the handling and use of corporate funds whether they are involved with cash or payments systems, receipts or dealing with contractors or suppliers;
- Reporting details immediately to their line manager or other avenue for reporting fraud (e.g. whistleblowing arrangements) if they suspect that fraud has been committed or see any suspicious acts or events.

Internal Audit

The role of internal audit is to deliver an opinion to the Accounting Officer on the whole of an organisation's risk management, control and governance. In relation to fraud this will include the examination of the adequacy of arrangements for managing the risk of fraud and ensuring that the organisation actively promotes an anti-fraud culture.

Internal audit will therefore assist in the deterrence of fraud by examining and evaluating the effectiveness of control commensurate with the extent of the potential exposure/risk in the various segments of an organisation's operations. Internal audit's main responsibility is to ensure that management has reviewed its risk exposures and identified the possibility of fraud as a business risk.

Management has the responsibility for conducting fraud investigations but internal audit may be asked to assist, and in some organisations may have had responsibility for conducting investigations delegated to them. Fraud investigation is an area that requires specialist knowledge and where internal audit has this responsibility they need to develop and maintain appropriate levels of expertise.

Appendix 2

Promoting an Anti-fraud Culture

Introduction

Fraud prevention involves more than merely compiling anti-fraud policies. It also involves putting in place effective accounting and operational controls and the maintenance of an ethical environment that encourages staff at all levels to actively participate in protecting public money and property. Creating an anti-fraud culture involves:

- Having a clear statement of ethical values;
- Establishing a clear anti-fraud policy and fraud response plan;
- Promoting staff awareness of fraud;
- Recruiting honest staff (checking references etc); and
- Maintaining good staff morale.

Code of Ethics

As stewards of public funds civil servants must have, and be seen to have, high standards of personal integrity. Staff should not accept gifts, hospitality or benefits of any kind from a third party that might be seen to compromise their integrity.

All personnel should be reminded that they are bound by a code of ethics which, unless issued separately, should be stated in the anti-fraud policy. The ethics policy will:

- Explain that staff must follow the organisation's rules without circumventing controls;
- Explain what external interests may give rise to conflicts of interest and require any possible conflicts of interest to be declared;
- Define the organisation's policy on receiving gifts from external parties;
- Explain why it is necessary to keep certain information about the organisation confidential;
- Require employees to report suspected fraud to a named individual or via a fraud hotline;
- State that breach of the policy will be treated as a disciplinary offence;
- Provide cross-references to the organisations anti-fraud policy and fraud response plan.

The seven principles of public life set out in the Nolan Committee's report on *Standards in Public Life* are relevant here.

The Seven Principles of Public Life

Selflessness	Holders of public office should take decisions solely in terms of the public interest. They should not do so in order to gain financial or other material benefits for themselves, their family, or their friends.
Integrity	Holders of public office should not place themselves under any financial or other obligation to outside individuals or organisations that might influence them in the performance of their official duties.
Objectivity	In carrying out public business, including making public appointments, or recommending individuals for rewards and benefits, holders of public office should make choices on merit.
Accountability	Holders of public office are accountable for their decisions and actions to the public and must submit themselves to whatever scrutiny is appropriate to their office.
Openness	Holders of public office should be as open as possible about all the decisions and action that they take. They should give reasons for their decisions and restrict information only when the wider public interest clearly demands it.
Honesty	Holders of public office have a duty to declare any private interests relating to their public duties and to take steps to resolve any conflicts arising in a way that protects the public interest.
Leadership	Holders of public office should promote and support these principles by leadership and example.

Fraud Policy

Many organisations use a **fraud policy** statement to communicate the organisation's approach to fraud. Such a statement may include some or all of the following areas:

- A statement about the organisation's attitude to fraud (e.g. zero tolerance);
- The Code of Ethics;
- Personnel policies (e.g. recruitment policies);
- The allocation of responsibilities for the overall management of fraud;
- Reporting suspicions of fraud, including "hotline" arrangements if used;
- Whistle blowing arrangements, including compliance with the Public Interest Disclosure Act;
- The procedures which staff should follow if a fraud is discovered;
- Guidance on training for the prevention and detection of fraud;
- Reference to the response plans that have been devised to deal with and minimise the damage caused by any fraudulent attack.

An example of a fraud policy statement can be found at **Appendix 3**.

Fraud Response Plan

It is important that managers and others know what to do in the event of a fraud so that they can act without delay. It is recommended that departments prepare a **fraud response plan**.

The objective of a fraud response plan is to ensure that timely and effective action can be taken to:

- Prevent losses of funds or other assets where fraud has occurred and to maximise recovery of losses;
- Minimise the occurrence of fraud by taking rapid action at the first signs of a problem;
- Identify the fraudsters and maximise the success of any disciplinary/legal action taken;
- Minimise any adverse publicity for the organisation, suffered as a result of fraud;
- Identify any lessons which can be acted upon in managing fraud in the future;
- Reduce adverse impacts on the business of the organisation;
- Make people aware of the possible consequences of committing fraud by publicising details of successful actions taken against perpetrators of fraud.

The existence of a fraud response plan may, in itself, help to act as a deterrent as it shows that an organisation is prepared to defend itself against the risk of fraud. **Appendix 4** contains more information about what to include in a fraud response plan.

Promoting Staff Awareness of Fraud

All staff need to be kept fully informed about the organisation's anti-fraud policy and what part they are expected to play in it. This can be achieved in a number of ways:

- Give every employee a copy of the organisation's ethics/anti-fraud policy as part of their contract of employment or staff handbook;
- Informing new staff during induction training;
- Establishing a training programme and ensuring all staff attend it;
- Making the anti-fraud policy, code of ethics and fraud response plan available to all staff (e.g. via networked IT systems);
- Communicating all changes in policy to staff immediately;
- Including fraud matters in a weekly or monthly newsletter;
- Reporting to staff outcomes of investigations and disciplinary action against employees who perpetrate theft or fraud.

Personnel Policies

Personnel recruitment policies play an important role in reducing the risk of fraud. Managers and staff responsible for staff recruitment must adhere strictly to the organisation's recruitment policy, particularly in relation to:

- The screening of references for new employees;
- Special arrangements for sensitive posts (e.g. checking police records);
- Detailed appraisal during probationary periods; and
- Detailed "exit" interviews for employees leaving the organisation.

Maintaining Staff Morale

Managers should try to create the conditions in which staff have neither the motivation nor the opportunity to commit fraud. The maintenance of good staff morale may help to minimise the likelihood of an employee causing harm to the organisation through fraud.

Appendix 3

Example of an Anti-fraud Policy

A fraud policy statement should be simple, focused and easily understood. It's contents may vary from organisation to organisation but you should consider including references to the organisation's determination to:

- Take appropriate measures to deter fraud;
- Introduce/maintain necessary procedures to detect fraud;
- Investigate all instances of suspected fraud;
- Report all suspected fraud to the appropriate authorities;
- Assist the police in the investigation and prosecution of suspected fraudsters;
- Recover from fraudsters any assets wrongfully obtained;
- Encourage employees to report any suspicion of fraud.

Source: The Fraud Advisory Panel's report "Fighting Fraud – A Guide for Small and Medium sized Enterprises"[9].

An example of an anti-fraud policy follows.

Introduction

The [**Organisation name**] requires all staff at all times to act honestly and with integrity and to safeguard the public resources for which they are responsible. The Department will not accept any level of fraud or corruption; consequently, any case will be thoroughly investigated and dealt with appropriately. The Department is committed to ensuring that opportunities for fraud and corruption are reduced to the lowest possible level of risk.

What is Fraud?

No precise legal definition of fraud exists; many of the offences referred to as fraud are covered by the Theft Acts of 1968 and 1978. The term is used to describe such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion.

"Fraud" is usually used to describe depriving someone of something by deceit, which might either be straight theft, misuse of funds or other resources, or more complicated crimes like false accounting and the supply of false information. In legal terms, all of these activities are the same crime – theft.

[9] www.fraudadvisorypanel.org

Avenues for Reporting Fraud

The Department has in place avenues for reporting suspicions of fraud. Staff should report such suspicions to their line managers, to the department's internal audit (or specialist fraud unit), or to the hotline set up for the purpose. All matters will be dealt with in confidence and in strict accordance with the terms of the Public Interest Disclosure Act 1998. This statute protects the legitimate personal interests of staff. Vigorous and prompt investigations will be carried out into all cases of actual or suspected fraud discovered or reported.

Responsibilities

Chapter 5 of Government Accounting 2000 sets out the responsibilities of departments in relation to fraud.

- The 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.
- Overall responsibility for managing the risk of fraud has been delegated to….. [e.g. the Principal Finance Officer (PFO)]. Their responsibilities include:
  - Developing a fraud risk profile and undertaking a regular review of the fraud risks associated with each of the key organisational objectives in order to keep the profile current;
  - Establishing an effective anti-fraud policy and fraud response plan, commensurate to the level of fraud risk identified in the fraud risk profile;
  - Developing appropriate fraud targets – SDA and/or PSA;
  - Designing an effective control environment to prevent fraud commensurate with the fraud risk profile;
  - Establishing appropriate mechanisms for:
    - reporting fraud risk issues;
    - reporting significant incidents of fraud to the AO;
    - reporting to Treasury in accordance with GA 2000 Chapter 5; and
    - coordinating assurances about the effectiveness of anti-fraud policies to support the Statement of Internal Control.
  - Liaising with the Risk Management Committee and/or Audit Committee.

- Making sure that all staff are aware of the organisation's anti-fraud policy and know what their responsibilities are in relation to combating fraud;
- Developing skill and experience competency frameworks;
- Ensuring that appropriate anti-fraud training and development opportunities are available to appropriate staff in order to meet the defined competency levels;
- Ensuring that vigorous and prompt investigations are carried out if fraud occurs or is suspected;
- Taking appropriate legal and/or disciplinary action against perpetrators of fraud;
- Taking appropriate disciplinary action against supervisors where supervisory failures have contributed to the commission of fraud;
- Taking appropriate disciplinary action against staff who fail to report fraud;
- Taking appropriate action to recover assets;
- Ensuring that appropriate action is taken to minimise the risk of similar frauds occurring in future.

Operational managers are responsible for:

- Ensuring that an adequate system of internal control exists within their areas of responsibility and that controls operate effectively;
- Preventing and detecting fraud;
- Assessing the types of risk involved in the operations for which they are responsible;
- Reviewing and testing the control systems for which they are responsible regularly;
- Ensuring that controls are being complied with and their systems continue to operate effectively;
- Implementing new controls to reduce the risk of similar fraud occurring where frauds have taken place.

Internal audit is responsible for:

- Delivering an opinion to the Accounting Officer on the adequacy of arrangements for managing the risk of fraud and ensuring that the department promotes an anti-fraud culture;
- Assisting in the deterrence and prevention of fraud by examining and evaluating the effectiveness of control commensurate with the extent of the potential exposure/risk in the various segments of the department's operations;
- Ensuring that management has reviewed its risk exposures and identified the possibility of fraud as a business risk;

- Assisting management in conducting fraud investigations.

Every member of staff is responsible for:

- Acting with propriety in the use of official resources and the handling and use of public funds whether they are involved with cash or payments systems, receipts or dealing with suppliers;
- Conducting themselves in accordance with the seven principles of public life set out in the first report of the Nolan Committee "Standards in Public Life". They are: selflessness, integrity, objectivity, accountability, openness, honesty and leadership;
- Being alert to the possibility that unusual events or transactions could be indicators of fraud;
- Reporting details immediately through the appropriate channel if they suspect that a fraud has been committed or see any suspicious acts or events;
- Cooperating fully with whoever is conducting internal checks or reviews or fraud investigations.

Fraud Response Plan

The department has a Fraud Response Plan that sets out how to report suspicions, how investigations will be conducted and concluded. This plan forms part of the department's anti-fraud policy.

Conclusion

The circumstances of individual frauds will vary. The department takes fraud very seriously. All cases of actual or suspected fraud will be vigorously and promptly investigated and appropriate action will be taken.

Appendix 4

Fraud Response Plans

A fraud response plan should cover the following areas:

- Instructions on the action required at the point of discovery;
- To whom the fraud or suspicion of fraud should be reported in the first instance, for example this may a line manager, the nominated "appeals" officer within a department, through internal procedures authorised by the employer (e.g. fraud hotline), internal audit department, anti-fraud specialists or exceptionally the Civil Service Commissioners;
- How the organisation should investigate the fraud and who will lead the investigation. Depending on the nature of the fraud special investigators, internal auditors who have been trained in fraud investigation, techniques or a fraud unit may be used. The facts should be established quickly by the operational managers; any threat of further frauds or losses should be removed immediately, for example, by changing procedures or suspending payments;
- How to secure evidence without alerting suspects at the outset of the investigation;
- How to secure the evidence in a legally admissible form (e.g. evidence must be carefully preserved; it should not be handled and no marks made on original documents; a record should be kept of anyone handling evidence);
- Guidance about dealing with employees under suspicion (e.g. prompt action must be taken; action to suspend or dismiss an employee should be taken in conjunction with the personnel department; employees under suspicion who are allowed to remain on the premises must be kept under constant surveillance; make an immediate search of the suspects work area, filing cabinets, computer files);
- Guidance about interviewing (e.g. decisions about interviewing suspects must be made by senior management; if the Police are to be used they must be involved at an early stage; all interviews must be conducted under properly controlled conditions in order to ensure that any statement taken and subsequently used as evidence in a court case will not be rejected as inadmissible; the guidelines and code of conduct for interviewing suspects issued under PACE should be applied);
- When and how to contact the Police. Any decision about involving the Police must be taken by senior management. A record of police contacts should be recorded in this section;
- Guidance about recovering assets (e.g. action to trace and freeze assets; action to prevent the release of assets; obtaining search orders);
- What experts to contact for advice (e.g. insurers, regulatory body, parent department, solicitors, accountants). There should be a list of these and contact details in this section. The right experts should be involved from the start;
- Advice about briefing those with responsibility for dealing with the media (e.g. must tell them precisely what information they can release, instruct them to maintain a record of what information was released and to whom);

- How to mitigate the threat of future fraud by taking appropriate action to improve controls;
- How to disseminate the lessons learned from the experience in cases where there may be implications for the organisation as a whole.

An effective fraud response plan should be closely tailored to each organisation's circumstances. It should reflect the likely nature and scale of losses.

Appendix 5

Detecting Fraud

Introduction

The Treasury's annual report on fraud perpetrated by civil servants consistently reveals that most frauds (over 50%) are discovered through **the normal operation of control procedures** and that **information from third parties** accounts for around 30% of cases. Other ways in which frauds are detected include:

- Suspicion;
- Accident;
- Internal/external audit;
- Confession; and
- Staff changes.

Normal Control Procedures

Well-designed and cost effective internal controls should identify a majority of actual or attempted frauds. Examples of good internal controls include:

- Supervision and checking output;
- Separation of duties to ensure that key functions and controls are not performed by the same member of staff;
- Random spot checks by managers;
- A complete and secure audit trail;
- Monitoring management information;
- Budgetary and other financial control;
- Independent reviews.

More examples of internal controls can be found in **Appendix 8**.

Information from Third Parties

Under the right conditions staff are themselves an excellent deterrent against fraud. There should be avenues for reporting suspicions of fraud. Staff should be encouraged to report suspicions of fraud either to their line mangers, to internal audit or possibly to a hotline set up for the purpose. It is important that staff know where to report their suspicions and that any suspicions of fraud reported in this way are seen to be acted upon by management. The Public Interest Disclosure Act 1998 protects whistleblowers that make responsible disclosures from dismissal and victimisation.

Members of the public should also be encouraged to report their suspicions of fraud through advertising campaigns, offering rewards, ensuring that avenues for reporting fraud are widely publicised and assuring whistleblowers that any information received will be treated confidentially.

Computer Assisted Audit Techniques

These can be used to identify unusual types of transaction within a department's records, which might be worth further investigation. Such checks could be built into information systems to provide regular exception reports to managers on transactions.

Investigation and Analysis Tools

These help fraud investigators to handle their case evidence, for example by highlighting links between colluding parties or between fraudulent transactions. These techniques can be used to identify indicators of possible fraud including:

- Duplicate payments;
- Unusual patterns of works orders (e.g. a large number of jobs valued just below the financial limits at which full competition in awarding the work would be employed);
- Invalid VAT numbers or incorrect amounts of VAT;
- Unexpected relationships between sub-contractors (e.g. shared addresses, telephones or fax numbers, bank accounts or directors).

Data mining is a technique that can be used to identify the relationships between sets of data within a department's databases. Some of the patterns identified may indicate fraudulent activity or practices that increase the risk of fraud.

Data matching can be used to compare computer records held for different purposes or by different bodies to identify discrepancies and anomalies. A department, for instance, could compare its data on contractors with similar data held by other public sector bodies to see who have committed fraud to see whether or not they are using the same firms.

Where organisations use data mining or data matching to detect fraud then they need to be aware of the possible restrictions on the way personal data can be used in fraud detection exercises or fraud investigations under the Data Protection Act 1998. The Office of the Information Registrar recommends the adoption of Codes of Practice setting out the measures to be adopted by those engaged in data matching. The purpose of such codes is to ensure that data matching exercises operate with appropriate safeguards to help protect individuals' privacy and to reduce the risk of failing to comply with the Data Protection Act. A "Guide to Developing Data Protection Codes of Practice on Data Matching" can be found on the Office of the Information Registrars website at: **www.dataprotection.gov.uk/match.htm**

Fraud Indicators

Fraud indicators are clues or hints that a closer look should be made at an individual, area or activity. All they can do is point the way for further detailed investigation. See **Appendix 6** for examples of fraud indicators.

Appendix 6

Examples of Fraud Indicators

A number of frauds can come to light because of suspicions aroused by, for instance, the behaviour of certain individuals. Managers and staff should also be alert to any warning signs that might indicate that fraud is taking place. These may be:

- Staff under stress without a high workload.
- First to arrive in the morning, last to leave at night.
- Egotistical (e.g. scornful of system controls).
- A risk taker or rule breaker.
- Reluctance to take leave.
- Refusal of promotion.
- Unexplained wealth.
- Sudden change of lifestyle.
- New staff resigning quickly.
- Cosy relationships with suppliers/contractors.
- Suppliers/contractors who insist on dealing with one particular member of staff.
- Disgruntled at work, a complainer.
- Greedy or has genuine financial need.

To spot fraud indicators in individual areas or activities it is important that accepted practices have been established for the area or activity under review and that the auditor is familiar with them. The following are examples of possible fraud indicators in a number of areas.

- 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 long-hours working, job dissatisfaction/unhappy employee, secretiveness or defensiveness).
- Key documents missing (e.g. invoices, contracts).
- Inadequate or no segregation of duties.
- Absence of controls and audit trails.
- Inadequate monitoring to ensure that controls work as intended (periodic testing and evaluation).
- Documentation that is photocopied or lacking essential information.
- Missing 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.
- Overdue pay or expense advances.
- General ledger out of balance.
- Duplicate payments.
- Ghost employees on the payroll.
- Large payments to individuals.
- Crisis management coupled with a pressured business environment.
- Lack of established code of ethical conduct.
- Lack of Senior Management oversight.
- Unauthorised changes to systems or work practices.
- Lack of rotation of duties.
- Policies not being followed.
- Post Office boxes as shipping addresses.
- 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 levels of review or approval.
- Vague specifications.
- Disqualification of any qualified bidder.
- Climate of fear or an unhealthy corporate culture.
- High staff turnover rates in key controlling functions.
- Chronic understaffing in key control areas.
- Low staff morale/lack of career progression/weak management.
- Excessive hours worked by key staff.
- Consistent failures to correct major weaknesses in internal control.
- Management frequently override internal control.
- When an employee is on leave, the work is left until the employee returns.
- Lack of common sense controls such as changing passwords frequently, requiring two signatures on cheques or restricting access to sensitive areas.
- An employee's lifestyle is more affluent than would be expected from his/her employment.

Appendix 7

Reducing Opportunities for Fraud

Introduction

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;
- By making it too much effort to commit.

Internal Control

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

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

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

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

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

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

Assets can range from the computer terminal that sits on the desk to the cheques sent out to pay suppliers. As a general principle all assets should be held securely and access to them restricted as appropriate. The control should apply not only to the premises but also to computers, databases, banking facilities, documents and any other area that is critical to the operation of the individual organisation. It may even be appropriate to restrict knowledge of the existence of some assets.

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

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

- Clear definition of the responsibilities of individuals for resources, activities, objectives and targets. This includes defining levels of authority. This is a preventive measure which sets a limit on the amounts which may be authorised by individual officers. To be effective, checks need to be made to ensure that transactions have been properly authorised;

- Establishing clear reporting lines and the most effective spans of command to allow adequate supervision;

- Separating duties to avoid conflicts of interest or opportunities for abuse. This is also largely a preventive measure which ensures that the key functions and controls over a process are not all carried out by the same member of staff (e.g. ordering goods should be kept separate from receipt of goods); similarly authorisation and payment of invoices; and

- Avoiding undue reliance on any one individual.

Supervision and checking of outputs: supervision is the function by which managers scrutinise the work and performance of their staff. It provides a check that staff are performing to meet standards and in accordance with instructions. It includes checks over the operation of controls by staff at lower levels. These act as both preventive and detective measures and involve monitoring theworking 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 8**

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. A department 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 departments can do this include:

- Warnings on forms such as: "false statements may lead to prosecution";
- General publicity;
- Increasing the severity of penalties;
- 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. Departments need to be clear about the objectives and targets of their campaigns.

Appendix 8

Risks and Controls in Specific Systems

Risks associated with 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 committed	Examples of controls
Theft	• Cash should be held securely at all times. • Access to cash should be restricted to named personnel. • Controls over keys should be set up and keys should only be issued to authorised personnel. • Cash balances should be kept to a minimum, recorded and checked periodically.
Income received not brought to account	• Always issue pre-numbered receipts. • Maintain accurate records of income received. • Post opening duties should be carried out by at least two people and a receipts log completed and signed by both officers. • Separate duties at key stages of the process: - post opening and logging of receipts; - bringing receipts to account and preparation of cash and cheques for banking; - daily cash balancing and bank reconciliations. • Regular and random management checks of source documentation, accounting records and bank reconciliations; • Rotation of staff.
Illegal transfer or diversion of money Changes and additions to payee details through BACS.	• Changes and additions to payee details and other standing data should be independently authorised. • System access to make and authorise these changes should be carefully restricted and logged. • Provide adequate supervision of all staff particularly new, inexperienced or temporary staff. • All payments should be independently authorised before they are made. • Restrict knowledge of transfer codes (and passwords if payments are initiated internally by computer) to approved personnel. Transfer codes and passwords should be changed frequently and always when staff leave.

How fraud could be committed	Examples of controls
	• Payment reports should be independently reviewed for accuracy immediately before the transfer of funds occurs. • Separation of duties between those setting up payment accounts and those authorised to trigger payments should be maintained at all times. Similarly separate duties of receiving goods and services from the process of making payment.
False creation of or unauthorised updates to accounting records to allow the unauthorised payment of funds.	• Amendments and deletions to accounting records should be independently authorised. These should be evidenced by signature, together with name and grade. • Independent checks to ensure amendments have been carried out correctly. These should be evidenced by signature, together with name and grade. • Authorisation levels and frequency of checks, including the use of spot checks, should depend on: - the amounts involved; - the degree of risk associated with the system. • Accounting records and petty cash should be reconciled on a regular basis. These reconciliations should be recorded and independently reviewed. Discrepancies should be investigated and resolved. • Any discrepancies that cannot be resolved, or any losses that have occurred should be reported as part of a formally defined process. • Suspense accounts should be reviewed on a regular basis to confirm their validity.
Falsification and duplication of invoices in order to generate a false payment.	• There should be segregation of duties between ordering and payment of invoices. • Checks for duplicate invoices should be carried out periodically. • Invoices should be checked back to orders for evidence that the orders were genuine and properly authorised.
Unauthorised use of cheques and payable orders.	• Financial stationery should be held securely and records kept of stock holdings, withdrawals and destruction of wasted stationery. • Signatories and delegated powers should be established for cheques and payable orders. • Cheques and payable orders should be checked to source documentation before issue. • Use restrictive crossings such as “non-transferrable” 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.

How fraud could be committed	Examples of controls
	• Discourage 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 £ sign 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 cheque listings regularly.

Risks associated with payroll

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 committed	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 employee grade.	• Ensure that, wherever possible, all other payroll changes are made by a personnel function that is organisationally separate from payroll function. Only Personnel should be able to autho rise changes to the payroll. • Ensure that all new appointments not subject to recruitment by a separate Personnel function (including part-time and casual staff) and changes to standing data (e.g. new pay rates) are approved and separately authorised by the employing department and by Personnel who should independently con firm the existence of starters and that rates of pay to be paid to starters are correct. • Produce listings of all starters, leavers and changes to standing data as part of every payroll run. At least a sample should be checked by Payroll section and a further random sample checked by management. • Produce regular exception reports (e.g. emergency tax codes for more than 6 months, no NI numbers, duplicate payees) for investigation by management. • Subject the payroll masterfile to periodic checks by personnel to ensure that each post is authorised, that the correct person is in post, that the person exists and that basis salaries and allowances are correct.
Making false claims for allowances, travel and subsistence.	• Establish a comprehensive set of travel and subsistence rules and ensure that they are communicated to staff.

How fraud could be committed	Examples of controls
	• 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 countersigning officers to initial and amendments to details on claim forms and finance teams to reject any claims where amendments have not been initialled. • Instruct finance teams to ensure that correct rates are claimed, substantiating documents (e.g. hotel invoices) are included and to compare counter signatures on claims against sample signatures provided by authorised countersignatories. • Random management checks should be carried out to verify details on claims and to ensure that finance team checks are applied rigorously to claims. • Budget holders should be provided with sufficient information to enable them to monitor travel costs against budget.

Risks associated with grant funding

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 committed	Examples of controls
Grant funds are misappropriated.	• Strict guidelines on the claims procedures should be established and communicated to all staff employed to process claims, especially new recruits. • Delegated authorities and levels of authorisation should be established. • Claims should be assessed to determine their complexity and level of risk and allocated accordingly to officers with the relevant experience and expertise. • All claims and supporting evidence should be checked for accuracy, completeness and timeliness. • No single officer should be involved in processing and authorising a complete claim and appropriatesegregation should be maintained throughout the process. • Good quality case records should be maintained. • An officer with the appropriate delegated authority should give the final approval for a claim.

How fraud could be committed	Examples of controls
	• Training needs should be assessed periodically and appropriate training plans drawn up. • All claims relating to an individual or organisation should be identified and cross-referenced to reduce the risk of duplicating payments. • Periodic reassessments should be carried out where on-going claims are concerned. • Copies of all outgoing correspondence should be traceable to the originating officer. • Liaise with other grant making organisations to check application data and to avoid making payments where the payment of other grants mean that claimants are not entitled to them. • Reports of grant payments should be regularly scrutinised to ensure that only approved grants have been paid out and that they have gone to the correct recipients. • Systems operated by organisations who receive grant funding for specific projects should be reviewed to ensure that the spending of grant monies is adequately controlled.

Risks associated with 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 committed	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. • Authorised signatories and their authorisation limits should be established for requisitioning and placing orders and adhered to. • Invoices should be authorised and matched to orders before the invoice is certified for payment. • Stock records should be maintained up to date so that stocks, stock usage and orders can be monitored. • There should be separation of duties between those ordering, receiving goods, and approving and paying invoices. This separation of duties should be reviewed regularly. • Authorised staff only make amendments to standing data such as the supplier records.

How fraud could be committed	Examples of controls
	• Budget holders should regularly check items of expenditure charged against their budgets. • Regular and random management checks should be carried out to confirm the existence of assets.
Short deliveries of goods or services may be accepted as a result of collusion.	• Random management checks that involve matching copy orders to delivery notes and goods should becarried out.
Acceptance of unsolicited goods or expanded orders as a result of fraudulent acceptance of attractions such as free gifts.	• Payment for goods should only be made after confirming that goods were properly ordered and authorised.
Misuse of Government Procurement Cards/ credit cards.	• Named individuals should be appointed as cardholders. • All purchases should be approved by the budget holder who should not also be a card-holder. • Use suppliers with whom the department has a contractual relationship or is otherwise a reputable merchant. • Departments should appoint an individual to be the cardholder manager who will be responsible for appointing cardholders and for dealing with the card-issuing bank. • The card-issuing bank should distribute the cards to a point in the department agreed with the departmental cardholder manager. The cardholder should sign the card in the presence of the card holder manager. The department should maintain an up to date list of all its cardholders. • Cards should only be issued by the bank upon request by the card holder manager. • Cards must be returned to the cardholder manager when card-holders move or cease to be cardholders. The cardholder manager should ensure that the card is destroyed and the record of cardholders amended. • Departmental policy and advice on using GPCs should be clearly documented, kept up to date and effectively communicated to all staff. • 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.
Orders placed on the Internet fail 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.

How fraud could be committed	Examples of controls
	• 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 sideof caution and remember that it may be difficult to seek redress if problems arise. • 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.

Risks associated with the use of contractors

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 committed	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. • Seek tenders from suitable suppliers (must comply with EC/GATT regulations). • Draw up clear and comprehensive tender evaluation criteria. • Tenders should be delivered to those responsible for selection without interference.

How fraud could be committed	Examples of controls
	• Late tenders should not be accepted. • Tenders should be evaluated by a tender evaluation board against the agreed evaluation criteria. • The tender that offers the best value for money should be recommended for acceptance. • The Project Board should approve the successful contractor. • Staff should be required to declare any personal interests they may have which may affect the tendering process.
Payments made for work not carried result of collusion between the contractor and official.	• Invoices are paid only when accompanied by independent certification that work has been been satisfactorily carried out. • There is a register of contracts in progress. • Contracts are only added to the contract register when properly approved and authorised. • Invoices are only accepted from approved contractors. • All contract variations are authorised, documented, variation orders are sequentially numbered, produced in an agreed format and authorised before payment. • Checks are made against budget and planned expenditure prior to approval of payment.

Risks associated with 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 committed	Examples of controls
Theft or unauthorised use of assets	• Asset register to be maintained up to date. Inventories to be used, where possible, and assets assigned to individual budget centres. • There is adequate definition of assets on the asset register. • Asset marking to be carried out where possible. • Physical security of assets to be maintained. • Spot checks on existence of assets to be carried out on a regular basis.

Risks associated with sensitive 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 committed	Examples of controls
Theft of sensitive/restricted documentation or information.	• All data should be stored securely and adequately backed up. • Personal data should be held in accordance with the Data Protection Act 1998 (e.g. fairly and lawfully processed; processed for specified purposes; not excessive; accurate; not held for longer than necessary; processed in line with data subject's rights; secure; not excessive, not transferred to countries where the rights of data subjects cannot be adequately protected). • Procedures should be in place to provide data subjects with access to data held about them in compliance with the Freedom if Information Act, and Human Rights Act). • Access to computer records should be logged and spot checks made to confirm that there were valid reasons for any unusual accesses. • Computer logs should be adequately protected against unauthorised access and amendment.