



HM TREASURY

Tackling Internal Fraud

January 2011



HM TREASURY

Tackling Internal Fraud

January 2011



Official versions of this document are printed on 100% recycled paper. When you have finished with it please recycle it again.

If using an electronic version of the document, please consider the environment and only print the pages which you need and recycle them when you have finished.

© Crown copyright 2011

You may re-use this information (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view this licence, visit <http://www.nationalarchives.gov.uk/doc/open-government-licence/> or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or e-mail: psi@nationalarchives.gsi.gov.uk.

ISBN 978-1-84532-823-8
PU1115

Contents

	Page
Foreword	3
Chapter 1 Introduction	5
Chapter 2 Understanding and Measuring Fraud Risks	7
Chapter 3 Creating and Maintaining the Right Structures and Culture to Combat Fraud	9
Chapter 4 Dealing with Fraud Risk	13
Chapter 5 Deriving Assurance over the Fraud-risk Strategy	19
Annex A Related Legislation	21
Annex B Anti-fraud Policy – Example	23
Annex C Fraud Response Plan Guidance	27
Annex D Fraud Indicators	29
Annex E Risks and Controls in Specific Systems	31
Annex F Money Laundering	37

Foreword

A recent estimate by the National Fraud Authority puts annual losses in the public sector due to fraud at around £25 billion. At a time when Government departments have to make significant cuts in spending, this level of loss is unsustainable and every effort should be made to cut fraud losses significantly.

A big challenge for departments during a period of significant reform and fiscal consolidation is to ensure that any major business change is delivered within a viable risk management and control framework. Fraud risk is always an important issue but in a period of considerable financial pressure the risk of fraud may increase for a number of reasons including:

- Job losses and the fear of redundancy can lead people to commit fraud;
- People are more likely to disregard internal control or engage in unethical business practices;
- Economic pressures may have a direct effect on people's ability to rationalise fraudulent actions;
- Staff reductions may mean fewer resources being spent on internal controls;
- Risk, compliance and assurance systems can be impacted by diminished investment; and
- Revised or new programmes may not have taken account of the risk of fraud.

This guide has been produced to help government bodies to meet these challenges. It covers the general principles of sound fraud risk management offering good practice advice to those with little or no knowledge of the subject. Although the emphasis of the guide is on the prevention and detection of internally generated fraud, many of the principles apply equally to reducing the risk of fraud by users of Government services.

We are grateful for the help of a number of central government bodies and other organisations, especially the National Fraud Authority, in producing this guide.

Chris Wobschall
Head, Assurance and Financial Reporting Policy
Head of the Government Internal Audit Profession
HM Treasury

1

Introduction

1.1 Departmental responsibilities in relation to the management of fraud risk are outlined in **Annex 4.7** of **Managing Public Money**¹. The purpose of this booklet is to expand on that advice and to show how the principles of sound risk management, governance and internal control apply to managing the risk of fraud and other irregular activities that might lead to fraud.

1.2 This guide provides general guidelines for managers and operational staff seeking to reduce the risk of fraud in an organisation. It provides guidance that can be applied to many aspects of government business including contracting, procurement, payroll, cash handling, grant payments and the management of assets and information. These principles apply equally to the management of fraud risk in the payment of benefits and collection of revenue for which there is specific guidance in the HM Treasury and NAO guide "tackling external fraud"².

1.3 The **term fraud** is commonly used to describe a wide variety of dishonest behaviours such as deception, bribery, corruption, forgery, false representation, collusion and concealment of material facts. It is usually used to describe the act of depriving a person of something by deceit, which may involve the misuse of funds or other resources, or the supply of false information. See also **Annex A** which covers some fraud-related legislation.

1.4 Fraud is just one of many risks an organisation faces. However, the deliberate nature of fraud can make it difficult to detect. Fraud risk is the vulnerability or exposure an organisation has towards fraud and irregularity. It combines the probability of fraud occurring and the consequent impact measured in monetary terms.

1.5 There are generally three main factors that can induce people to perpetrate a fraud:

- The reward from the fraud is perceived to outweigh the risk;
- The individual may rationalise of the act on the grounds of a personal grievance or set of circumstances ; and
- The opportunity to carry out the fraud presents itself or the likelihood of detection is perceived as unlikely.

1.6 While some people would never contemplate perpetrating a fraud, others might be tempted if they thought they could avoid detection, particularly at a time when some might consider that the risk of detection is reducing. An organisation requires the ability to prevent, detect, and investigate fraud and pursue sanctions to deter potential fraudsters.

1.7 The removal of the opportunity is generally the simplest action for managers trying to minimise the risk of fraud. Opportunities to commit fraud may be reduced by ensuring that a sound system of control, proportionate to risk, has been established and that it is functioning as intended.

1.8 In times of fiscal hardship, where pay and rewards are constrained, staff with a personal grievance may feel more inclined to justify irregular actions. Communications campaigns are

¹ http://www.hm-treasury.gov.uk/psr_mpm_index.htm

² <http://www.hm-treasury.gov.uk/fraud>

examples of trying to set a positive cultural environment. A clear lead from top management on the ethical standards expected of staff and the creation of a positive work environment can significantly reduce the likelihood of fraud being rationalised.

1.9 The risk of fraud is ever present but in times of austerity there may be more need to direct resources at this risk. The risk of fraud can increase for a number of reasons including:

- Economic pressures have a direct effect on people's perceived economic circumstances and could increase the likelihood that they engage in fraudulent activity;
- Staff reductions may result in fewer internal controls such as separation of duties, approval processes, supervision and rotation of staff;
- Risk and compliance systems can be impacted by diminished investment;
- Revised or new programmes may not have taken sufficient account of the risk of fraud.

1.10 In broad terms managing the risk of fraud involves:

- Understanding and measuring fraud risks (**Chapter 2**);
- Creating and maintaining the right structures and culture to combat fraud (**Chapter 3**);
- Dealing with fraud risk (**Chapter 4**); and
- Delivering assurance over the fraud-risk strategy (**Chapter 5**).

2

Understanding and Measuring Fraud Risks

Introduction

2.1 The potential for fraud can be considered as a set of risks to be managed alongside other risks. Preventive controls and the creation of the right type of corporate culture will help to reduce the likelihood of fraud occurring while detective controls and effective contingency planning can reduce the size of any losses.

2.2 A risk-based approach enables organisations to target their resources more efficiently. Before designing expensive controls to reduce the risk of fraud, it is important to know the extent to which an organisation is vulnerable to fraud. This involves:

- Assessing the organisation's overall vulnerability to fraud which should be considered as part of an overall risk assessment;
- Identifying the areas most vulnerable to fraud risk; and
- Evaluating the scale of fraud risk.

Assessing the Organisation's Overall Vulnerability to Fraud

2.3 Fraud risks are often considered as part of an organisation-wide risk assessment programme although they may be addressed separately. The extent to which an organisation carries out a fraud-risk assessment will depend on the size and complexity of the organisation and nature of its activities.

2.4 Where there are complex delivery arrangements, or organisations are dependent upon delivery partners or Arms Length Bodies, it may be appropriate to gauge the level of fraud risk in those bodies and seek commensurate assurances.

Identifying the Areas Most Vulnerable to Fraud

2.5 A high-level consideration of fraud risk will determine whether there are areas that are vulnerable to fraud and will help to decide if there is a need to perform a more detailed fraud-risk assessment. It will not be cost effective to cover every possible threat situation therefore the likely occurrence of fraud and the impact on key organisational objectives must be assessed. This stage involves:

- Identifying the processes or activities at risk of fraud (e.g. through commissioning a risk review, undertaking risk self-assessments, issuing questionnaires, benchmarking/ comparisons with other organisations).
- Assessing and ranking the nature and extent of vulnerability in each area. Some common criteria/factors used to make judgements about vulnerability include:
 - Overall size, scope and value of activities, as well as the nature, security and value of assets held;

- Adequacy of operational controls (e.g. separation of duties, supervision, approval, staff rotation) including appropriate skills/knowledge of supervisory staff;
- The particular forms of fraud threat to each area (e.g. theft, fraudulent administration of contracts, falsification of source records such as timesheets);
- Extent of effective reporting mechanisms and the ability to stop frauds occurring quickly;
- Degree of operational complexity and impact of technology;
- The quality, reliability and adequacy of staffing arrangements including recruitment processes; and
- Adverse motivational factors that could induce staff to commit fraud.

Evaluating the Scale of Fraud Risk

2.6 In deciding how to address the fraud risks identified, it is important to evaluate their significance. Risk evaluation and assessment will inform decisions about the areas of risk and the relative priority of those risks where action needs to be taken. 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. The risk assessment should consider the financial impact, the potential political and commercial sensitivities involved and the likely effect on the organisation's reputation. The analysis should be both qualitative and quantitative. The qualitative approach usually involves grading risks in high, medium or low categories.

3

Creating and Maintaining the Right Structures and Culture to Combat Fraud

Introduction

3.1 All government departments and agencies have a responsibility to develop anti-fraud policies to show those seeking to defraud the government that such action is unacceptable and will not be tolerated. The annual Statement on Internal Control will have considered the adequacy of the arrangements for managing risks, including that of fraud.

Establishing a clear anti-fraud policy (see Appendix B)

3.2 Many organisations use a fraud policy statement to communicate the organisation's determination to address fraud. Such a statement should be simple, focused and easily understood and may include some or all of the following areas:

- 1 A statement about the organisation's fraud strategy;
- 2 The allocation of responsibilities for the overall management of fraud;
- 3 Reporting suspicions of fraud, including "hotline" arrangements if used;
- 4 The development of an anti-fraud culture including a code of ethics.

Fraud Strategy

3.3 An organisation's fraud strategy should:

- Set out clear goals (e.g. zero tolerance) and what this means in terms of deterring and detecting fraud, investigating cases and pursuing sanctions;
- Set the level of financial investment in work to combat fraud in proportion to the risk that has been identified;
- Provide those tasked with countering fraud with the necessary authority and support;
- Ensure that those working to counter fraud have the training and accreditation they need.

Allocating Responsibilities

3.4 Everybody in an organisation contributes to the management of fraud risk. The Accounting Officer has overall responsibility and is accountable for the effectiveness of fraud-risk management. Specific responsibility for managing the risk of fraud may be allocated to an appropriate senior officer, preferably at board level, such as the Finance Director (FD).

3.5 For major financial transaction processing systems, FDs may be supported in this role by Process Owners who provide a view of the risks end-to-end. Responsibility for the day-to-day management of specific fraud risks should be allocated to appropriate operational managers.

3.6 Internal audit¹ is responsible for providing the Accounting Officer with an objective evaluation of, and opinion on, the overall adequacy and effectiveness of the organisation's framework of governance, risk management and control. The Head of Internal Audit's opinions are a key element of the framework of assurance that the Accounting Officer needs to complete the annual Statement on Internal Control (SIC). In carrying out its work, internal audit must be alert to the possibility of significant errors, fraud or non-compliance. It is a management responsibility to put in place procedures to deter, detect and investigate fraud, and internal audit can help assess the adequacy of the control framework.

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

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

Establishing Appropriate Avenues for Reporting Suspicions of Fraud and System Vulnerabilities

3.8 Staff are the first line of defence in combating fraud. There should be avenues for reporting suspicions of fraud or concerns about control weaknesses that could be exploited for fraudulent purposes. Staff should be encouraged to report suspicions to their line managers or to a hotline set up for the purpose. It is important that staff know where to report their suspicions, that any suspicions reported in this way are seen to be acted upon by management and to assure those who report their suspicions that any information received will be treated confidentially. Information on reported suspicions should routinely be made available to internal audit.

3.9 Of interest in this area is the Public Interest Disclosure Act². The Act provides remedies for workers who are dismissed or subject to detriment for making responsible disclosures. It should also help encourage a climate of greater openness and accountability in dealing with fraud within organisations. It does this by providing some protection to whistleblowers from unfair dismissal and victimisation. More advice on the Act can be found on the "Public Concern at Work" website³.

Anti-fraud Culture

3.10 The creation and maintenance of an anti-fraud culture is critical to maximising the engagement of employees in combating fraud. Creating an anti-fraud culture involves:

¹See also the HM Treasury guide "Fraud and the Government Internal Auditor" at http://www.hm-treasury.gov.uk/d/fraud_internal_auditor_250510.pdf

²http://www.opsi.gov.uk/acts/acts1998/ukpga_19980023_en_1

³<http://www.pcaaw.co.uk/>

- **Senior managers setting the right tone.** Tone at the top is set by the Accounting Officer and Board members who must behave ethically and communicate their expectations for ethical behaviour to staff in the organisation.
- **Having a clear statement of ethical values.** As stewards of public funds, civil servants must have, and be seen to have, high standards of personal integrity. The seven principles of public life (selflessness, integrity, objectivity, accountability, openness, honesty, and leadership) set out in the Nolan Committee's report on Standards in Public Life are important here. All personnel should be reminded that they are bound by a code of ethics (see also the **Civil Service Code – Annex 4.2 of Managing Public Money⁴**) that, unless issued separately, should be stated in the anti-fraud policy. The ethics policy should:
 - 1 Explain that staff must follow the organisation's rules without circumventing controls;
 - 2 Explain that external interests may give rise to conflicts of interest and require any possible conflicts of interest to be declared;
 - 3 Define the organisation's policy on receiving gifts from external parties;
 - 4 Explain why it is necessary to keep certain information about the organisation confidential;
 - 5 Require employees to report suspected fraud or money laundering to a named individual or to a fraud hotline;
 - 6 State that breach of the policy will be treated as a disciplinary offence;
 - 7 Provide cross-references to the organisations anti-fraud policy and fraud response plan.
- **Maintaining good staff morale.** A positive workplace environment improves staff morale and loyalty. 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.

⁴ http://www.hm-treasury.gov.uk/psr_mpm_index.htm

4

Dealing with Fraud Risk

Introduction

4.1 Tackling fraud requires holistic action across:

- Prevention and Detection;
- Deterrence; and
- Investigation, Sanction and Redress.

Prevention and Detection

4.2 In respect of fraud risks, prevention is almost always preferable to detection. The strongest defence is a sound system of internal control. In designing controls, it is important that the control put in place is proportionate to the 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 audit is an important source of advice on the range of appropriate controls to assist management in preventing and detecting fraud. Examples of internal controls can be found in [Appendix E](#).

4.3 The Treasury's annual report on fraud perpetrated by staff consistently revealed that most fraud was discovered through the normal operation of control procedures or as a result of information received from staff or members of the public.

Data Analytics and Data Sharing

4.4 With the growing sophistication of fraud, many organisations are looking to take a more proactive approach, in particular through the use of data analytics. Data analytics is the common term used to describe the process of bringing the necessary data together to verify and validate transactions, or to uncover potential and actual fraud. The ability to gather, store and make sense of ever-expanding amounts of data in real-time has opened up the possibility of combating fraud while at the same time enhancing the customer experience.

4.5 The application of data analytics for fraud prevention encompasses:

- Real-time credit reference and other data checks.
- On-line verification techniques.
- Data matching with data held by other public and private sector organisations, and
- Predictive/innovative analytics, which involves developing a model to score data for potential fraud and error, which can then forecast probabilities of fraud and error to an acceptable level of reliability.

4.6 The same processes of data analytics can be used to detect fraud. The National Fraud Initiative (NFI) is an effective data matching exercise currently run by the Audit Commission. It compares information held by different organisations and within different parts of an organisation to identify potentially fraudulent claims and overpayments. The NFI 2008-09

identified fraud, overpayment and errors with a value of £215 million. Currently, around 1,300 public and private sector organisations take part.

4.7 Data analytics relies on the sharing of data and fraud intelligence between government bodies and with the private sector to prevent (and detect) fraud¹. Government bodies need to carefully consider a number of issues before deciding whether or not to share data.

Considerations include:

- Will the sharing of information benefit the organisation?
- Are there any barriers to the sharing of data (e.g. Data Protection Act)? The Information Commissioner's Office recommends the adoption of their "Code of Practice for Sharing Personal Information"².
- Will the organisations with which data might be shared provide assurances that information will be stored securely and only used for agreed purposes?

4.8 The Serious Crime Act 2007 provides one of a number of legal gateways permitting public authorities to enter into data sharing arrangements with certain Specified Anti-fraud Organisations (SAFOs) (an anti-fraud organisation is one which enables, or facilitates, any sharing of information to prevent fraud).

4.9 The Home Office has produced a Code of Practice for public authorities disclosing information under sections 68 to 72 of the Serious Crime Act 2007 to a specified anti-fraud organisation³. In the Foreword to the Code, the Information Commissioner advises: "the powers under the Act must be considered in the context of any Data Protection Act requirements. Specifically, information must be shared in a manner that is proportionate, and any organisations must take steps to ensure that they only share such data as is necessary for the prevention of fraud.

4.10 Where organisations engage in information sharing, being transparent and enabling individuals to exercise their rights to know how their information is being used is crucial. Equally, the security of information is a major priority. Organisations sharing data need to define and agree the detail around what data will be shared and how any data protection risk will be minimised"

4.11 Organisations should maintain records of suspected or confirmed fraud. This record should capture information for individual cases such as the type or category of the fraud, the control weaknesses that were exploited, the actions taken to correct the weaknesses and actions against the perpetrators of the fraud. It is good practice to report this to the Audit Committee on a regular basis.

Staffing Issues

4.12 Staff (including permanent staff, temporary/agency staff, contractors etc) have privileged access to an organisation's assets. Their participation in the various processes through which departments function are critical for business delivery. This also provides opportunities to commit fraud. Although the vast majority of staff are honest, a small number of individuals exploit their status to commit fraud. Some individuals will also try to secure a position within an organisation with the intention of committing fraud.

¹ See the report of the Smarter Government Public Sector Fraud Taskforce published in March 2010 -

<http://www.attorneygeneral.gov.uk/nfa/WhatAreWeSaying/Pages/fraud-news-march10-smarter-government-public-sector-fraud-task-force-report.aspx>

² http://www.ico.gov.uk/for_organisations/topic_specific_guides/information_sharing.aspx

³ http://www.whatdotheyknow.com/request/2971/response/7150/attach/3/12761_290510%20Data%20Sharing.pdf

4.13 Anyone in the organisation presents a potential fraud risk regardless of their position, age, gender or length of service, although the type of, and level of risk, will vary according to their position in the organisation in relation to the type of assets a staff member has access to or the processes they are involved in. Many frauds are opportunistic in nature. However, organised crime groups regard staff in many organisations as a valuable commodity and seek to exploit insider information and assistance in serious and organised crime.

4.14 A number of factors may motivate staff to use their positions to commit fraud and enable them to rationalise doing so. Financial stress is one key motivating factor but other factors could include fear of failing to meet performance standards, peer, family or community pressure or feelings of being treated unfairly by the organisation. Equally, they may be under external pressure by, or exploited by, a crime syndicate.

4.15 HR controls can help to combat this type of fraud:

- **Staff screening⁴.** Screening policies play an important role in reducing the risk of fraud.
 - It is important to assess the fraud risk associated with sensitive posts so that proportionate response measures can be put in place⁵. The level of screening of staff should relate directly to the level of fraud risk inherent in the position they (will) occupy.
 - Screening/vetting produces only a ‘snapshot’ picture at a particular point in time. The majority of corrupt employees were not corrupt at the time they were recruited and circumstances change over time. Repeat screening should be considered dependent on the level of risk. Screening also needs to be applied with the movement of staff between posts within the organisation.
- **Recruitment procedures.** Managers responsible for staff recruitment must adhere strictly to the organisation’s recruitment policy, particularly in relation to:
 - The screening of references for new employees, including temporary staff such as consultants and contractors;
 - Detailed appraisal during probationary periods.
 - Clarity on where responsibility lies for screening of contractor/agency staff etc and explicit requirements. Lack of clarity on responsibility can lead to staff not being screened at all.
- **Proportionate action against corrupt staff.** Organisations should not simply allow corrupt staff to resign to avoid investigation/sanction. Procedures should also be in place for Human Resources to notify the designated counter-fraud contact of any disciplinary actions where fraud is involved.
- **Structured “exit” interviews for employees leaving the organisation.** Staff leaving the organisation may have information on issues and weaknesses within the organisation.

⁴ For detailed guidance, see <http://www.cabinetoffice.gov.uk/media/45160/baseline-personnel-security-standard.pdf>

⁵ For detailed guidance see http://www.cpni.gov.uk/Docs/Risk_Assessment_Pers_Sec_Ed_2.1.pdf

Fraud Indicators

4.16 Fraud indicators are clues or hints that a closer look should be made at an individual, area or activity. 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 reviewers are familiar with them. Examples of issues that could be investigated to ensure fraud is not taking place can be found in [Appendix D](#).

Deterrence

4.17 Deterrence involves eliminating the factors that might cause fraud in particular to stop the rationalisation of the act. Organisations actively need to create a strong deterrent effect through communicating:

- The commitment of the organisation to combat fraud;
- The effectiveness of existing prevention and detection arrangements including successful results;
- The determination of the organisation to pursue sanctions and redress.

4.18 It is very important to target potential fraudsters with key messages. Publicity should be integrated into plans, initiatives and specific cases to have the maximum impact on the intended audience. The goal should be to change attitudes and behaviours towards fraud.

Investigation, Sanctions and Redress

4.19 For the investigation of fraud, an organisation needs to make sure that:

- Any investigative work is effective and there is a system in place for assessing this;
- Investigations are carried out in accordance with clear guidance;
- Those who undertake investigations have been trained in fraud investigation techniques and have the necessary powers, both in law, where necessary, and within the organisation;
- Referrals are handled and investigations are undertaken in a timely manner;
- There is 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.

4.20 The overall investigation process may involve:

- Maintaining confidentiality;
- Identifying assets (to freeze and hopefully recoup losses);
- Protecting evidence;
- Interviewing witnesses and people under suspicion;
- Dealing with the police;

- Managing civil proceedings (e.g. to recover assets);
- Liaising with experts and regulators;
- Preparing media statements;
- Reporting progress and findings to senior management.

4.21 Departments should have a fraud response plan place (an example is attached at **Annex C**).

4.22 For sanctions and redress, an organisation needs to put in place policies and procedures that provide:

- A clear and consistent policy on the application of sanctions where fraud or corruption is proven to be present;
- The consideration of all possible sanctions – disciplinary/regulatory, civil and criminal;
- Monitoring of the extent to which the application of sanctions is successful;
- A clear policy on the recovery of losses incurred;
- An effective approach to recovering any losses incurred by fraud and the ability to monitor the recovery of these losses.

5

Deriving Assurance over the Fraud-risk Strategy

5.1 It is important that organisations seek regular assurances over the effectiveness of their fraud-risk strategies. Assurance should be monitored at board level and is a core component of the Statement on Internal Control process. It can be derived from a number of sources:

- Front-line business, in terms of evidence that policies, processes, controls and checks are in place and working effectively. Mechanisms could include monitoring statistics and indicators. This would feature in director's stewardship reporting arrangements and could incorporate elements of control risk self-assessment;
- A secondary line of assurance can come from separate arrangements that management has put in place to assure itself that things are operating as they should be. In relation to fraud-risk management it could include the results of regular and continuous monitoring by risk and compliance specialists or quality assurance reviewers;
- Within the third line of defence, internal audit provides an organisation with independent and objective assurance on the framework of risk management, control and governance. As part of this work, internal audit should be alert to the potential risks of fraud and periodically review the organisation's capability to manage the risk of fraud as a discrete subject area.

5.2 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.

5.3 Success can be measured by focusing on the real outcomes achieved from the key actions outlined in the strategy. The outcomes to be measured could include the following:

- Fraud awareness levels;
- Reports of suspicions;
- Successful investigations;
- Sanctions applied;
- Financial losses recovered and where appropriate financial savings;
- Reductions in levels of fraud both in terms of numbers of cases and the overall value of losses.

Continuously Monitoring the Fraud-risk Environment

5.4 The risk environment is constantly changing and priorities of objectives and the consequent importance of risks on the fraud risk profile will shift and alter. Risk models have to be regularly revisited and reconsidered in order to derive 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.

Fraud Risk in Policy Development

5.5 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. When designing and implementing new policies, programmes and systems it is important to ensure that good controls are built in to reduce the risk of fraud where appropriate. Expert advice on fraud-risk management should be sought (e.g. from internal audit or counter fraud specialists) early in the process and at key stages during design and implementation. Where innovative schemes are being proposed, it is good practice to pilot these to identify any further risks of fraud. An early evaluation of the controls is helpful in determining whether risk measures have been effective in countering fraud risks during and at various stages during the life of the project, programme or system.

Fraud in Online Systems

5.6 Specific attention should be given to the risk of fraud in online services. As government services, and in particular citizen-facing services, move online, it will be important to ensure the appropriate counter-fraud measures are in place from the beginning. Expert advice on fraud-risk management should be sought (e.g. from internal audit or counter fraud specialists) early in the process and at key stages during design and implementation.

Delivery Partners

5.7 In organisations where some key front-line services are delivered by, or supported by, third parties, it is important that the organisation is satisfied that services are delivered in line with its fraud policy and that it receives appropriate assurances that counter fraud controls have been established and are operating effectively.

A

Related Legislation

UK Fraud Act 2006

A.1 The UK Fraud Act 2006¹ came into force on 15 January 2007. This establishes that the offence of fraud can be committed in three ways:

- False representation (section 2);
- Failing to disclose information (section 3);
- Abuse of position (section 4).

A.2 It is no longer necessary to prove that a victim was deceived. All that is required is to prove that the fraudster was dishonest in their behaviour and that they intended to make a gain for themselves or cause a loss to another (e.g. the dishonest builder who conducts repairs that are unnecessary; dishonest representation made in an application in order to secure a job).

A.3 The offence of fraud by abuse of position could include dishonest conduct by agents. If an agent dishonestly abuses their position, with a view to making a gain for themselves or intending to make a loss for another, or to expose the other party to risk of loss, then that agent will have committed an offence. Fraud under this section of the Act may also arise by deliberate omission rather than by dishonest act or acts.

A.4 Separate offences are committed under the Act if a party is in possession of articles for use in fraud. These could range from computer hardware/software to information for the purpose of identity theft. It is a separate offence to make or supply articles for use in fraud. A new offence of obtaining services dishonestly is also introduced by the Act, for example, downloading software dishonestly.

Scottish Law

A.5 Scotland has a common law offence of fraud which is committed when someone achieves a practical result by false pretence. There is also a separate offence of 'uttering' whereby an article, usually a document, is passed off as genuine to the prejudice of another person.

Bribery Act

A.6 The **Bribery Act 2010**² was introduced in the Queen's Speech to Parliament on 18 November 2009. The bill received Royal Assent on 8th April 2010.

A.7 The Act defines four new criminal offences:

- Offering or paying a bribe;
- Requesting or receiving a bribe;

¹ http://www.opsi.gov.uk/acts/acts2006/pdf/ukpga_20060035_en.pdf

² <http://www.legislation.gov.uk/ukpga/2010/23/contents>

- Bribing a foreign public official; and
- A corporate offence of failing to prevent bribery being undertaken on its behalf. Where wrongdoing is uncovered, a corporate entity will automatically be guilty of an offence, unless it can demonstrate that it had “adequate procedures” in place to prevent bribery.

A.8 The act defines ‘bribery’ in wide terms, to capture the differing ways in which bribes are made or received. It sets out several scenarios, or “cases”. The one which is expected to apply to most businesses is the offence of giving a bribe, specifically: “the defendant offers, promises or gives a financial or other advantage intending to induce another person to perform improperly one of their functions in their position of trust and responsibility, or as a reward for improper performance”.

A.9 The legislation applies to all companies, partnerships and individuals based in England, Scotland, Wales and Northern Ireland, as well as foreign companies and individuals doing business in the UK. It has a global reach, applying to acts or omissions taking place anywhere in the world.

Other Relevant Acts

A.10 Other legislation referred to in this guide include:

- Terrorism Act 2000;
- Proceeds of Crime Act 2002;
- Money Laundering Regulations 2003 (see also **Annex F**);
- Public Interest Disclosure Act 1998;
- Serious Crime Act 2007; and
- Data Protection Act 1998.

B

Anti-fraud Policy – Example

Introduction

B.1 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 minimised.

What is Fraud?

B.2 The term "fraud" is commonly used to describe a wide variety of dishonest behaviour such as deception, forgery, false representation, and concealment of material facts. It is usually used to describe the act of depriving a person of something by deceit, which may involve the misuse of funds or other resources, or the supply of false information.

Avenues for Reporting Fraud

B.3 The Department has in place avenues for reporting suspicions of fraud or money laundering. 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

B.4 Annex 4.7 of Managing Public Money sets the general responsibilities of departments in relation to fraud.

B.5 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.

B.6 Managing fraud risk will be seen in the context of the management of this wider range of risks.

B.7 Overall responsibility for managing the risk of fraud has been delegated to... [e.g. the Finance Director (FD)]. 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 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 their suspicions of fraud or money laundering;
- Taking appropriate action to recover assets;
- Ensuring that appropriate action is taken to minimise the risk of similar frauds occurring in future.

B.8 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.

B.9 Internal audit is responsible for providing the Accounting Officer with an objective evaluation of, and opinion on, the overall adequacy and effectiveness of the organisation’s framework of governance, risk management and control.

B.10 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 or money laundering;
- Reporting details immediately through the appropriate channel if they suspect that fraud or money laundering 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

B.11 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

B.12 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.



Fraud Response Plan Guidance

C.1 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 or money laundering should be reported in the first instance, for example this may be 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 who have been trained in fraud investigation techniques or a fraud unit should 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.

C.2 An effective fraud response plan should be closely tailored to each organisation's circumstances. It should reflect the likely nature and scale of losses.

D

Fraud Indicators

D.1 Fraud indicators are clues or hints that a closer look should be made at an individual, area or activity. Examples of issues that could be investigated to ensure fraud is not taking place include:

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

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

E

Risks and Controls in Specific Systems

Cash handling

E.1 There are many risks associated with cash handling. Theft or misappropriation of cash may be assisted by the suppression, falsification or destruction of accounting records, or where no initial records are created at all. This section suggests some controls that should be in place.

How Fraud Could be Perpetrated	Examples of Controls
Theft	<ul style="list-style-type: none"> ▪ Hold cash securely at all times. ▪ Restrict access to cash to named personnel. ▪ Hold keys securely and limit access to authorised personnel. ▪ Keep cash balances to a minimum. ▪ Maintain transaction records. ▪ Carry out periodic and independent checks and reconciliations.
Income received not brought to account	<ul style="list-style-type: none"> ▪ Issue pre-numbered receipts (ideally receipts should be generated automatically); ▪ Maintain prompt and accurate records of income received. ▪ Ensure post-opening duties are carried out by at least two people and receipts log completed and signed by both officers. ▪ Separate duties at key stages of the process: <ul style="list-style-type: none"> ○ bringing receipts to account and preparation of cash and cheques for banking; ○ daily cash balancing and bank reconciliations. ▪ Establish regular and random management checks of source documentation, accounting records and bank reconciliations; ▪ Rotate staff duties frequently.
Illegal transfer or diversion of money. Changes and additions to payee details through BACS.	<ul style="list-style-type: none"> ▪ Ensure that changes and additions to payee details and other standing data are properly authorised. ▪ Restrict and log system access to make and authorise these changes. ▪ Provide adequate supervision of all staff particularly new, inexperienced or temporary staff. ▪ Ensure payments are authorised before they are made. ▪ Restrict knowledge of transfer codes (and passwords if payments are initiated internally by computer) to approved personnel. ▪ Change transfer codes and passwords frequently and always when staff leave. ▪ Ensure that payment reports are independently reviewed for accuracy immediately before the transfer of funds occurs. ▪ Separate duties (e.g. between those setting up payment accounts and those authorised to trigger payments and between those receiving goods and services and those who process and make payment).
Accounting records are falsified or amended to allow unauthorised payments.	<ul style="list-style-type: none"> ▪ Ensure that amendments and deletions to accounting records are authorised. ▪ Carry out independent checks to ensure amendments have been made correctly. ▪ Establish authorisation levels. ▪ Perform frequent independent checks, including spot checks. ▪ Reconcile accounting records and petty cash frequently, maintain reconciliation records and carry out independent reviews. Investigate and resolve all discrepancies. ▪ Report any discrepancies that cannot be resolved, or any losses that have occurred. ▪ Regularly review suspense accounts to confirm their validity.
Invoices are falsified or duplicated in order to generate false payment.	<ul style="list-style-type: none"> ▪ Segregate duties between ordering and payment of invoices. ▪ Carry out routine checks: <ul style="list-style-type: none"> ○ Invoice has a genuine purchase order number; ○ Match invoice to purchase order and goods received note ; ○ Check invoice detail looks right, that amounts and calculations are correct etc; ○ Ensure invoice had not already been paid, by checking relevant records.
Supplier bank account details are changed in order to divert payments.	<ul style="list-style-type: none"> ▪ Only accept requests for changes to supplier standing data in writing. ▪ Seek confirmation from the supplier that the requested changes are genuine using contact details held on the vendor data file or from previous and legitimate correspondence. Do not contact the supplier via contact details provided on the letter requesting the changes. ▪ Ensure that there is segregation of duties between those who authorise changes and those who make them. ▪ Maintain a suitable audit trail to ensure that a history of all transactions and changes

How Fraud Could be Perpetrated	Examples of Controls
	<ul style="list-style-type: none"> are maintained. ▪ Produce reports of all changes made to supplier standing data and check that the changes were valid and properly authorised before any payments were made. ▪ Regularly verify the correctness of standing data with suppliers.
Unauthorised use of cheques and payable orders.	<ul style="list-style-type: none"> ▪ Hold financial stationery securely and maintain records of stock holdings, withdrawals and destruction of wasted stationery. ▪ Establish signatories and delegated powers for cheques and payable orders. ▪ Reconcile cheques and payable orders to source documentation before issue. ▪ Use restrictive crossings such as "non-transferable" and "a/c payee". ▪ Ensure that addresses to which payable instruments are sent are correct. For large value payments check encashment to ensure that the intended recipient did receive the payment. ▪ 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.

Payroll/Travel & Subsistence

E.2 Risks that may be associated with the payroll function include the introduction of non-existent (ghost) employees, unauthorised amendments made to input data, and the payment of excessive overtime, bonus or travel claims. This section suggests some controls that should be in place.

How Fraud Could be Perpetrated	Examples of Controls
Creating fictitious employees whose pay is then obtained by the fraudster or by someone in collusion, or obtaining pay that is not consistent with the employee's grade.	<ul style="list-style-type: none"> ▪ Ensure that only authorised personnel are able to update payroll records. ▪ Segregate duties between those responsible for authorising appointments and those who make changes to standing data and action payments. ▪ Produce listings of all starters, leavers and changes to standing data as part of every payroll run and check that all changes have been made correctly. ▪ Produce 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 master file to periodic checks by HR to ensure that each post is authorised, that the correct person is in post, that the person exists and that basic salaries and allowances are correct. ▪ Provide budget holders with sufficient and timely information to enable them to reconcile staffing costs against budget.
Making false claims for allowances, travel and subsistence.	<ul style="list-style-type: none"> ▪ Establish a comprehensive set of rules and ensure that they are communicated to staff. ▪ Establish a formal process that involves line managers approving and reviewing work plans and programmes for visits, especially for staff where there is no countersigning requirement. ▪ Institute checks by countersigning officers of claims against approved work plans, standard mileages for regular destinations and primary evidence such as hotel bills, rail tickets and taxi receipts. ▪ Ensure that countersigning officers pass approved claim forms direct to the finance team. ▪ Instruct finance teams to ensure that correct rates are claimed; substantiating documents (e.g. hotel invoices) are included and check that authorised claims were received from approved counter-signing officers. ▪ Establish random sample management checks to verify details on claims and to ensure that finance team checks were applied rigorously to claims. ▪ Provide budget holders with sufficient information to enable them to monitor costs against budget.
Misuse of Corporate Credit Cards	<ul style="list-style-type: none"> ▪ Establish clear policy/rules and communicate to all staff. ▪ Make one person or central group responsible for issuing cards (e.g. payments section). ▪ Authorise all card issues. ▪ Maintain a record of cardholders. ▪ Establish monthly credit limits. ▪ Require cardholders to submit expense claims regularly supported by invoices/receipts to the group that process payments for checking and reconciliation to card issuer statements. ▪ Ensure that cards are returned and destroyed when staff move or cease to be cardholders.

Grant payments

E.3 This section sets out examples of the controls that should be in place to counter the fraud risks specifically associated with payment of grants:

How Fraud Could be Perpetrated	Examples of Controls
Grant funds are misappropriated.	<ul style="list-style-type: none"> ▪ Establish clear guidelines on claims procedures and communicate to all staff employed to process claims, especially new recruits. ▪ Establish delegated authorities and levels of authorisation. ▪ Assess claims to determine their complexity and level of risk and allocate accordingly to officers with the relevant experience and expertise. ▪ Check all claims and supporting evidence for accuracy, completeness and timeliness. ▪ Maintain good segregation of duties throughout the process (e.g. approval, processing, payment authorisation, payment). ▪ Maintain good quality case records should be maintained. ▪ Assess training needs periodically and draw up appropriate training plans. ▪ Check claims by individuals to previous claims to reduce the risk of duplicating payments. ▪ Carry out Periodic reassessments on on-going claims. ▪ Liaise with other grant making organisations to reduce the risk of making payments where the payment of other grants mean that claimants are not entitled to them. ▪ Scrutinise reports of grant payments regularly to ensure that only approved grants have been paid out and that they have gone to the correct recipients. ▪ Review systems operated by organisations who receive grant funding for specific projects to ensure that the spending of grant monies is adequately controlled.

Purchasing

E.4 Risks associated with the operation of purchasing systems include the false input of invoices, the diversion of payments and misappropriation of purchases. This section sets out some examples of controls that should be in place to reduce the risk of fraud in this area:

How Fraud Could be Perpetrated	Examples of Controls
Unauthorised use of purchasing systems in order to misappropriate goods or use services for personal gain.	<ul style="list-style-type: none"> ▪ Restrict opportunity to generate payment by using sequentially numbered purchase order forms for all orders; perform independent checks to show that purchase orders are valid and accounted for. ▪ Establish authorised signatories and authorisation limits for requisitioning and placing orders. ▪ Match Invoices with orders before the invoice is certifying for payment. ▪ Keep stock records up to date so that stocks, stock usage and orders can be monitored. ▪ Separate the duties between those ordering, receiving goods, and approving and paying invoices. This separation of duties should be reviewed regularly. ▪ Ensure that authorised staff make amendments to standing data (e.g. supplier records). ▪ Provide budget holders with sufficient and timely information to enable them to reconcile expenditure against budget.
Short deliveries of goods or services	<ul style="list-style-type: none"> ▪ Check delivery notes to original orders, chase up short deliveries, and only pay for goods received.
Acceptance of unsolicited goods or expanded orders as a result of fraudulent acceptance of attractions such as free gifts.	<ul style="list-style-type: none"> ▪ Confirm goods were properly ordered, authorised and received before authorising payment. Only pay for goods ordered.
Misuse of Government Procurement Cards.	<ul style="list-style-type: none"> ▪ Establish a clear GPC policy that is communicated to all staff and should include expenditure limits for individual transactions. ▪ Appoint an individual to be the cardholder manager who will be responsible for appointing cardholders and for dealing with the card-issuing bank. ▪ Maintain a list of authorised cardholders. ▪ Cardholders should maintain a log of all transactions that should be supported by authorisations to make purchases, invoices/receipts. ▪ Cardholders must hold cards securely. ▪ Cardholders must check all entries on statements supplied by the bank and refer any discrepancies to the cardholder manager. ▪ Budget holders should carry out periodic checks to ensure that GPC statements are properly reconciled and that only authorised purchases are made. ▪ Ensure that cards are returned to the cardholder manager when cardholders move or cease to be cardholders. The cardholder manager should also ensure that the card is destroyed and the record of cardholders amended.
Orders placed on the Internet are not delivered or goods received are not of the desired quality.	<ul style="list-style-type: none"> ▪ Make sure your browser is set to the highest level of security notification and monitoring. ▪ Check that you are using the most up to date version of your browser and ensure their security features are activated. ▪ Keep a record of the retailer's contact details, including a street address and non-mobile telephone number. Beware if these details are not available on the website. Do not rely on the e-mail address alone. ▪ Click on the security icon to see if the retailer has an encryption certificate. This should

How Fraud Could be Perpetrated	Examples of Controls
	<p>explain the type and extent of security and encryption it uses. Only use companies that have an encryption certificate and use secure transaction technology.</p> <ul style="list-style-type: none"> ▪ If you have any queries or concerns, telephone the company before giving them your card details to reassure yourself that the company is legitimate. ▪ Print out your order and consider keeping copies of the retailer's terms and conditions and returns policy. Be aware that there may well be additional charges such as postage and VAT, particularly if you are purchasing goods from traders abroad. When buying from overseas always err on the side of caution and remember that it may be difficult to seek redress if 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.

Contracting

E.5 The section sets out some examples of controls which should be in place, in addition to those which apply generally to cash handling and purchasing systems, to counter the fraud risks faced in relation to the use of contractors:

How Fraud Could be Perpetrated	Examples of Controls
A contractor could be selected as a result of favouritism or who does not offer best value for money.	<ul style="list-style-type: none"> ▪ 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. ▪ Arrange for tenders to be delivered to those responsible for selection without interference. ▪ Do not accept late tenders. ▪ Ensure that tenders are evaluated against the agreed evaluation criteria by a tender evaluation board. ▪ The Project Board should approve the successful contractor. ▪ Require staff should to declare any personal interests they may have which may affect the tendering process.
Payments made for work not carried out as a result of collusion between contractor and official.	<ul style="list-style-type: none"> ▪ Ensure that invoices are supported by independent certification that work was performed satisfactorily before authorising payment. ▪ Maintain a register of contracts in progress. ▪ Only add approved and authorised contracts to the register. ▪ Accept invoices from approved contractors only. ▪ Ensure that all contract variations are supported by sequentially numbered and authorised variation orders before payment.

Assets

E.6 Risks in this area include use of assets for personal gain, or misappropriation of assets. This section suggests some controls that should be in place to counter those risks.

How Fraud Could be Perpetrated	Examples of Controls
Theft or unauthorised use of assets.	<ul style="list-style-type: none"> ▪ Maintain up to date asset registers and inventories ▪ Ensure that assets are assigned to individual budget centres. ▪ Clearly describe assets in registers and inventories. ▪ Mark assets in some way (e.g. property of HM treasury). ▪ Store assets securely. ▪ Carry out regular spot-checks to confirm existence of assets.

Information

E.7 The final section deals with some of the controls that should be in place to reduce the threat of fraud or other irregularities arising from access to sensitive information or misuse of information for private gain.

How Fraud Could be Perpetrated	Examples of Controls
Theft of sensitive/restricted documentation or information.	<ul style="list-style-type: none"> ▪ Identify all information assets. ▪ Produce a clear information risk policy and communicate to all staff. ▪ Implement the Government Mandatory Minimum Measures¹ for managing information risk. ▪ Define key roles and responsibilities for managing information risk (e.g. Senior Information Risk Owner, Information Asset Owners) and allocate to named individuals. ▪ Establish an effective information risk governance framework. ▪ Ensure that data security arrangements are underpinned by a culture that values and protects data. ▪ Carry out regular assessments of the information risks and whenever changes occur to technology or new threats are identified. ▪ Restrict access to information on a need to know basis. ▪ Ensure that access rights are reviewed regularly and that these are removed for staff that leave. ▪ Limit the use of removable media (e.g. laptops, USB memory sticks, CDs). Encrypt data transferred to removable media. ▪ Do not use e-mail to transmit confidential information unless it is encrypted. ▪ Regularly check the activities of those with rights to transfer personal or sensitive data to ensure that they continue to have a business case for these activities. ▪ Ensure that all data users successfully undergo information-risk awareness training. ▪ Ensure that contingency arrangements (so that damaged or lost data can be renewed or replenished quickly) are regularly tested. ▪ Put in place arrangements to log activities of data users and for managers to review usage. Computer logs should be adequately protected against unauthorised access and amendment.

¹ http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/dhr/cross_gov080625.pdf

F

Money Laundering

Introduction

F.1 Current money laundering legislation places the burden for identifying acts of money laundering on organisations and their employees. The main obligations are contained in the Proceeds of Crime Act 2002¹, the Terrorism Act 2000² and the Money Laundering Regulations 2003³. These Acts broaden the definition of money laundering and increase the range of activities caught by the statutory control framework. The definition of money laundering includes possessing, or in any way dealing with, or concealing the proceeds of any crime, whether committed by a body or an individual. In particular, criminal sanctions can be imposed for failure to report suspicions of money laundering.

What is Money Laundering?

F.2 Money laundering is the term used for a number of offences involving proceeds of crime or terrorist funds. The term goes beyond the transformation of the proceeds of crime into money or assets. The term also covers a range of activities, which do not necessarily need to involve money. Examples include:

- Concealing, disguising, converting, transferring criminal property or removing it from the UK (section 327);
- Entering into or becoming concerned in an arrangement which a person knows or suspects facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person (section 328); or
- Acquiring, using or possessing criminal property (unless there was adequate consideration) (section 329);
- An attempt, conspiracy or incitement to commit such an offence;
- Aiding, abetting, counselling or procuring such an offence;
- Becoming concerned in an arrangement facilitating concealment, removal from the jurisdiction, transfer to nominees or any other retention or control of terrorist property (section 18 of the Terrorist).

F.3 “Criminal property” is widely defined as a person’s benefit from criminal conduct. It includes all property, real or personal (situated in the UK or abroad), including money, and also includes an interest in land or a right in relation to property other than land. It does not matter how small the value of the benefit is.

¹ http://www.opsi.gov.uk/acts/acts2002/ukpga_20020029_en_1

² http://www.opsi.gov.uk/acts/acts2000/ukpga_20000011_en_1

³ <http://www.england-legislation.hmso.gov.uk/si/si2003/20033075.htm>

F.4 “Terrorist property” means money or other property that is likely to be used for the purposes of terrorism, proceeds of the commission of acts of terrorism, and acts carried out for the purposes of terrorism.

F.5 The broad definition of money laundering means that potentially anybody could contravene the money laundering offences if they become aware of, or suspect the existence of, criminal or terrorist property, and continue to be involved in the matter without reporting their concerns.

Money Laundering Offences

F.6 There are three principal offences:

- **Concealing** is where someone knows or suspects a case of money laundering, but conceals or disguises its existence.
- **Arranging** is where someone involves himself or herself in an arrangement to assist in money laundering.
- **Acquisition** is where someone seeks to benefit from money laundering by acquiring, using or possessing the property concerned.

F.7 There are also two ‘third party’ offences:

- **Failure to disclose** one of the three principal offences;
- **Tipping off** - where someone informs a person or people who are, or are suspected of being, involved in money laundering, in such a way as to reduce the likelihood of their being investigated, or prejudicing an investigation.

F.8 All the money laundering offences may be committed by an organisation or by the individuals working for it. Whilst it is considered most unlikely that a member of staff would commit one of the three principle offences, the failure to disclose a suspicion may be a serious offence (failure to disclose a suspicion is an offence if the suspicion relates to an actual crime).

Impact on Central Government Bodies

F.9 The Money Laundering Regulations apply to bodies whose activities, wholly or partly, constitute “relevant business” within the meaning of regulation 2(2) of those regulations. It is for each Government body to determine if it performs relevant business.

F.10 Departments carrying out such relevant business are required to have internal reporting procedures (regulation 7) including a Money Laundering Reporting Officer (MLRO) to receive money laundering reports and make reports to the Serious Organised Crime Agency (SOCA); to maintain certain identification procedures (regulation 4) and record-keeping procedures (regulation 6); and to establish other appropriate procedures for the purpose of forestalling or preventing money laundering (regulation 3(1)(b)). They are also required to train their employees in those procedures and, more generally, in the recognition of money laundering transactions and the law relating to money laundering (regulation 3(1)(c)). A relevant business, which fails to maintain the procedures or carry out the training, is guilty of a criminal offence (regulation 3(2)).

F.11 Departments who are neither in the regulated sector (for Proceeds of Crime Act purposes), nor engaged in “relevant business” (for money laundering regulation purposes) may however wish to act as if they were bound by the money laundering regulations. This decision should be based on a risk assessment of their organisation being one that could be used for money laundering. If the risk is high then the department may wish to consider appointing a Money Laundering Reporting Officer and putting in place systems for compliance with the other requirements of the money laundering regulations. Such nominated officers however would not

be criminally liable because of a Crown exemption under the Act (except for the Director of National Savings and his staff who can be prosecuted for breach of Part 7 of the Act).

F.12 External auditors (e.g. the National Audit Office) are now required to report, where they know or suspect, or have reasonable grounds to know or suspect, that money laundering has taken place where information has come to them during the normal course of business.

HM Treasury contacts

This document can be found in full on our website at:
hm-treasury.gov.uk

If you require this information in another language, format or have general enquiries about HM Treasury and its work, contact:

Correspondence Team
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

Tel: 020 7270 4558

Fax: 020 7270 4861

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

ISBN 978-1-84532-823-8



9 781845 328238 >