

Fraud report 2006-07: an analysis of reported fraud in Government departments

October 2007



HM TREASURY



HM TREASURY

**Fraud report 2006-07:
an analysis of reported fraud in
Government departments**

October 2007

© Crown copyright 2007

The text in this document (excluding the Royal Coat of Arms and departmental logos) may be reproduced free of charge in any format or medium providing that it is reproduced accurately and not used in a misleading context. The material must be acknowledged as Crown copyright and the title of the document specified.

Any enquiries relating to the copyright in this document should be sent to:

Office of Public Sector Information
Information Policy Team
St Clements House
2-16 Colegate
Norwich
NR3 1BQ

Fax: 01603 723000

e-mail: HMSOlicensing@opsi.x.gsi.gov.uk

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 and Enquiry Unit
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

Printed on at least 75% recycled paper.

When you have finished with it please recycle it again.

ISBN 978-1-84532-363-9

PU417

CONTENTS

	Page
Executive Summary	3
Chapter 2 Main Analyses	5
Chapter 3 Fraud Risk Management in Central Government	13
Annex A Analysis of Anti-fraud Questionnaires	17
Annex B Large Value Frauds Perpetrated by Staff	19
Annex C Large Value Frauds Perpetrated by Outsiders	23
Annex D Fraud Issues	27
Annex E Anti-fraud Initiatives	35

EXECUTIVE SUMMARY

1. 26 departments reported 1,067 cases of internal fraud or theft with losses totalling some £3,858,600. The main observations are:

- The biggest categories in terms of case numbers reported were theft of assets (403 cases) and personnel management related fraud (253 cases). A majority of cases in the latter category involved little or no direct financial loss to departments.
- In value terms two categories dominated: payment fraud (over £2.5 million) and theft of assets (over £512k). The payment fraud category included one case with a loss of £1.2million and 4 further cases, each exceeding £100k, accounted for losses of over £1million.
- Fraud relating to pay and allowances accounted for 122 cases with losses totalling £407k. One travel and subsistence fraud resulted in a loss of £126k and was perpetrated over a sustained period.

2. A comparison of the analysis of this year's anti-fraud questionnaires with that of the previous two years revealed a steady increase in the proportion of Government bodies that have processes in place to manage certain fraud risks effectively. There were some minor potential problem areas but overall, fraud risk is taken seriously in central government and managed effectively.

3. Information provided by government bodies in the anti-fraud questionnaires about new measures implemented during the year to reduce the risk of fraud are summarised in annex E. This summary provides a number of good examples of anti-fraud management that might be considered by others.

4. Control issues identified that Government bodies might bear in mind when reviewing their control processes included:

- Staff with too many key responsibilities;
- Insufficient monitoring by supervisors of staff with key responsibilities;
- Weak or no security over assets or information;
- Inadequate security checking of potential contractors, consultants or agency staff.

2

MAIN ANALYSES

This section contains the main analyses of data relating to fraud and theft by staff reported by departments for the year 2006-07.

INTRODUCTION

2.1 The purpose of this Report is to inform departments of the scale and nature of certain categories of fraud which have been reported to the Treasury for the reporting year 2006-2007. This information is provided to help departments learn from the experiences of others when reviewing and developing their own control systems. The Report also aims to increase awareness of the risk of fraud and, in some areas, to suggest ways in which the risk can be managed and reduced. **Annex E** provides summaries of activities undertaken by some departments in recent years to reduce the risk of fraud which also contain useful lessons for others.

2.2 The Report analyses data submitted by central Government departments and their agencies about fraud and theft perpetrated by staff. It also includes details of some fraud cases perpetrated by members of the public or contractors with a value of £20,000 or more and containing generic lessons for others (see **Annexes B and C**). **Annex D** provides some useful information about key fraud issues which might have an impact on anti-fraud activities in central government.

2.3 The Report does not set out to be a complete record of all internal theft or fraud perpetrated against central Government bodies and cannot be regarded as a definitive account of all frauds affecting Government during the relevant period. The Assurance, Control and Risk (ACR) team in the Treasury collates the data reported by departments. ACR applies care and judgement where necessary to ensure, as far as possible, that the report is based on a consistent analysis and classification. During 2007-08, the ACR team in conjunction with a number of departments will be carrying out a formal review of the Treasury publication "**Managing the Risk of Fraud – a Guide for Managers**".

2.4 In the past year, the Government has introduced some significant changes in the way that the problem of fraud is dealt with. In particular, the new Fraud Act 2006 came into force on 15 January 2007 in England and Wales. This clearly defines separate offences by which fraud can be committed, and focuses on the perpetrator's dishonest behaviour, rather than relying, as previously, on the degree of deception. This represents an entirely new way of investigating the many methods by which fraud can be perpetrated. During the year the findings of the Government's Fraud Review was published. This proposes a series of new measures intended to provide greater focus and improvements in both the national response to fraud, by the police, civil authorities, and the courts. More information on these new initiatives is provided in **Annex D**.

OVERVIEW

2.5 The analysis in this section is based on fraud data supplied by 45 central Government bodies, including all the main departments, covering the period 1 April 2006 to 31 March 2007. Overall the analysis shows:

- 19 bodies did not report any cases.
- The remaining 26 bodies reported 1067 cases of internal fraud or theft with a total value of £3,858,600.
- Overall there was an increase of 387 cases over last year's total of 789. The increases occurred in 3 large departments that had introduced improved processes for reporting fraud. The overall value of fraud and theft reported was reduced from last year's total by £1,250,800.
- There were 15 large value cases (£20,000 or more) accounting for a total loss of £2,710,400 (70% of total losses reported). Six of these cases each exceeded £100,000 in value with losses totalling £2,335,000 (61%) and included 1 case where losses exceeded £1million.
- The analysis of anti-fraud questionnaires (**Annex A**) found that most organisations had effective measures in place to manage fraud risk although more could be done to raise staff awareness of fraud, vet potential new staff, share information with other Government bodies and fraud proof new policies and programmes.

ANALYSIS OF FRAUD DATA

2.6 The following paragraphs provide analyses of the business areas in which the frauds/thefts were perpetrated.

Fraud Category	Cases		Value	
	Number	%	£	%
Travel, Subsistence & Other Allowances	69	6.47	245,000	6.35
Pay or Allowances Paid Via the Payroll	53	4.97	162,300	4.21
Theft of Assets	403	37.77	512,100	13.27
Exploiting Assets and Information	49	4.59	9,800	0.25
Procurement Fraud	10	0.94	56,800	1.47
GPC/Credit Card Fraud	36	3.37	27,800	0.72
Personnel Management Related Fraud	253	23.71	21,800	0.56
Payment Fraud	84	7.87	2,504,900	64.92
Receipt Fraud	74	6.94	281,000	7.28
Other	36	3.37	37,100	0.96
Total	1067		3,858,600	

PAYMENT FRAUD

2.7 These are frauds that involve falsely creating or diverting payments. Examples of cases reported included:

- Creating bogus customer records and bank accounts in order to generate false payments;
- Intercepting cheques and Payable Orders and attempts to cash them. In some cases alterations are made to payee details and amounts;
- Creating false records to support fraudulent claims for benefits;
- Processing false claims by accomplices for benefits, grants or repayments;
- A member of staff authorising payments to himself.

2.8 This is the largest category in terms of value lost (£2,504,900 or 65%) from 84 cases. Individual losses were sometimes significant with 5 cases (each exceeding £100,000 in value) accounting for losses totalling £2,209,000 (88% of total losses in this category).

2.9 Many of the large value frauds arose because individuals with key responsibilities worked largely unsupervised, allowing the frauds to go undetected for a time. These cases highlight the importance of rotating duties and effective monitoring where other controls such as segregation of duties cannot easily be implemented. Once someone is in a position to affect the processing of payments, they can pose a significant risk. It is not just payments to suppliers that are at risk. Central Government staff may be in a position to affect grant and benefit payments as well as collecting and administering taxes.

2.10 Segregation of duties, adequate audit trails, meaningful and regularly produced management reports, good budget management, regular management or independent reviews (e.g. by internal audit) and the secure holding of blank or completed instruments of payment are all examples of the basic controls that can be applied to the payment process. The wider use of electronic forms of payment might also reduce the risk of payment fraud. Collusion can be a difficult problem to deal with but the active encouragement of staff to report their suspicions of fraud and the deterrent effect of always taking appropriate action against known perpetrators can help reduce this risk. Appendix 8 of “Managing the Risk of Fraud – a Guide for Managers” offers advice about the controls that should be in place to help prevent or detect fraud in this area and Treasury’s Fraud Casenotes provide advice on controlling cash handling, bill paying, electronic funds transfer and payment by cheque or Payable Order.

THEFT OF ASSETS

2.11 This category relates to the theft of physical assets, including cash. Many cases arose because of weak security but some were opportunistic thefts (e.g. items such as laptops or mobile phones stolen from peoples’ desks), demonstrating the importance of storing such items securely at all times when not in use.

2.12 In total, departments reported 403 cases (38%) of thefts with a total value of £512,100 (13%).

2.13 This is a high-risk area and was the highest category in terms of number of cases reported and second highest in terms of value. However, no cases were reported this year where individual losses exceeded £20,000 in value.

2.14 It is important to focus on the basic physical controls that should prevent and detect these kinds of offences. These fundamental controls include asset registers, and inventories; regular checks and reconciliation of holdings; secure storage and movement of valuable items; and effective control of exit and entry to Government sites. Where mobile phones are stolen, it is important to identify the thefts quickly and to take prompt action to minimise losses due to their illegal use.

RECEIPT FRAUD

2.15 Fraud in this area can include the theft of incoming cash or cheques (which can be opportunistic or coupled with the manipulation of financial records to disguise thefts) or adjusting records of amounts owed by customers to departments in return for cash rewards or other incentives.

2.16 The overall value of fraud in this category was £281,000 involving 74 cases. This is a big increase over last year's figures of 19 cases with losses totalling £144,100. In one case, £25,000 was stolen over a period of time and involved the manipulation of accounting records. The fraud occurred because systems checks were not routinely carried out.

2.17 The scale of income collected by the Government is vast and individual frauds can potentially be very significant. It is important that accurate debtor records are maintained, that regular management and independent checks are carried out to ensure that income is collected and brought to account and that the work of officers with responsibility for pursuing large value debts is adequately supervised. Segregation of duties between those who raise debts, those who pursue them and those who bring payments to account together with good audit trails and management information will also help to reduce the risk of fraud in this area.

TRAVEL & SUBSISTENCE, PAY AND OTHER ALLOWANCES

2.18 Fraud in this area involves such activities as the completion of fraudulent claims for payment or the creation of false payroll records. Examples of fraud include claims for journeys that were not made, overstated claims, claims for allowances for which there was no entitlement, forged signatures authorising payment, forged documentation supporting claims or applications for employment, falsification and/or unauthorised amendments of timesheets, false claims for working unsociable hours, deliberate failure to repay salary overpayments and the creation of non-existent personnel on payrolls

2.19 In total there were 122 cases (69 travel & subsistence, 53 payroll frauds) with losses totalling £407,300 (11%). There was a big increase in the value of fraud reported in these categories over last year's combined total of £94,300. Two cases accounted for much of the increase: one where losses totalling £120,000 occurred over a long period because the system made it difficult to check travel claims easily; the other involved losses of over £87,500 where three staff members took unpaid leave and continued to receive their salaries for periods of 16, 21 and 24 months respectively.

2.20 Controls to prevent or detect fraud in this area are straightforward (e.g. clear set of rules, an approval process, management checks, finance team checks, spot checks and monitoring via the budgetary control process). To overcome collusion, good management checks and rotation of duties might reduce this risk. The key controls relating to travel and subsistence can be found in Treasury's Fraud Casenote Number 4 and in appendix 8 of Treasury's publication "Managing the Risk of Fraud – a Guide for Managers".

PROCUREMENT FRAUD & GPC/CREDIT CARD FRAUD

2.21 Procurement is the whole process of acquisition from third parties and covers goods, services and construction projects. Procurement fraud can involve contractors, sub-contractors, Crown Servants or any combination of these often colluding to perpetrate a fraud or act of corruption. These categories cover tendering irregularities, unauthorised or irregular use of the Government Procurement Card (GPC) and payment claims for goods or services that were not delivered.

2.22 These two categories accounted for 46 (4%) cases of fraud with a total value of £84,600 (2%). This included 36 GPC/credit card frauds with losses totalling £27,800. One procurement case accounted for losses of £35,000 and involved a member of staff ordering IT equipment for his own use. The fraud was discovered as a result of good budgetary control processes.

2.23 Examples of controls to reduce risks associated with purchasing or associated with the use of contractors can be found in Appendix 8 of Treasury's publication "Managing the Risk of Fraud – a Guide for Managers".

PERSONNEL MANAGEMENT RELATED FRAUD

2.24 Examples of fraudulent activities reported under this category included:

- Staff on sick leave but working elsewhere;
- Abuses of flexible working time systems;
- Misuse of official time (e.g. abusing the department's computer misuse policy);
- Deceit or misrepresentation for advantage (e.g. false references or false qualifications used to secure employment).

2.25 The second highest number of cases (253, 24%) was reported under this category but most involved little or no financial loss to the departments concerned. In all cases action had been taken against perpetrators that included dismissals, demotions, and loss of spine points and/or bars on promotion.

2.26 Whilst these cases are usually low-risk in terms of value, it is nevertheless important that departments try to detect them as staff who get away with this type of fraud may be tempted to attempt much more serious frauds. They can also reflect badly on a department's ethical standards. Closer checking of data supplied in order to gain employment, more frequent management checks of sick leave records, close scrutiny of flexible working hours records and independent monitoring of staff accesses to official data are all examples of controls designed to detect these types of frauds.

EXPLOITING ASSETS AND INFORMATION

2.27 This type of fraud involves using the assets of the organisation for other than official purposes and/or supplying information to outsiders for personal gain. Many of these cases had no reported value, as assessing losses is not always possible. Departments are required to report only those cases where the action taken against perpetrators goes beyond the oral or written stage (e.g. dismissal, downgrading, promotion bar).

2.28 This year departments reported 49 cases (5%) in this category with losses totalling less than £10k. This is potentially a high risk area as was demonstrated last year by one case where losses totalled £1,250,000 and involved a Government employee providing details of departmental records to an external accomplice to perpetrate the fraud.

2.29 Clear rules about how assets can be used, appropriate segregation of duties, effective audit trails, effective supervision of employees and regular management checks on the existence and use of assets can be effective in discouraging or preventing the misuse of assets or information. Good detective controls such as staff reporting their suspicions (there will need to be clearly advertised avenues for staff to do this), the use of IT checks (e.g. data mining or data matching) to provide indicators that fraud might be occurring and spot checks of claims for large refunds (e.g. tax and VAT) from members of the public can also be effective.

OTHER FRAUD

2.30 This category accounted for 36 cases (3% of the total) and a total value of £37,100 (1%). There were no high-value cases (i.e. £20,000 or more) reported.

EXTERNAL AND CONTRACTOR FRAUDS

2.31 Departments are asked to report any high value (i.e. £20,000 or more) external frauds including fraud perpetrated by contractors that contain lessons for other bodies. These are not included in the main analyses above (which do, however, include any cases involving staff working in collusion with outsiders).

2.32 In all, 16 external fraud cases were reported with losses totalling nearly £2.2million. Summaries of individual cases can be found in Annex C. This annex does not represent a complete record of all fraud perpetrated by contractors or members of the public against Government. Most external fraud is related to the main work of individual departments (e.g. benefit payments) and these cases are not reported to us for this exercise because they contain lessons for those departments only, and may be covered in other reports and publications.

2.33 Seven contractor cases were reported with losses totalling more than £740,000. All of these were contractors engaged to deliver services on behalf of departments to the public and in most cases losses had been, or were likely to be, recovered. In some cases the frauds arose because of weak controls such as insufficient checking of evidence to support claims for payment by the contractors. The 9 external cases included one case involving the theft of over £1m over a 9 year period by those responsible for managing the finances of people with reduced mental capacity, and arose because of a lack of control and little fraud awareness among those responsible for supervision. Thefts of blank payable instruments were also reported, which resulted in losses of over £120,000, as were cases involving the interception of completed payable instruments, altering

amounts and attempts to cash them (which were all picked up by banking controls before any losses occurred).

2.34 Advice on managing external fraud risk effectively can be found in the joint Treasury and NAO publication “Good Practice in Tackling External Fraud”¹.

¹ http://www.hm-treasury.gov.uk/documents/public_spending_reporting/governance_risk/psr_managing_risk_of_fraud.cfm

3

FRAUD RISK MANAGEMENT IN CENTRAL GOVERNMENT

This section contains an analysis of questionnaires on the management of the risk of fraud completed by 244 central Government bodies. This section also summarises the main new controls/processes put in place by central government bodies in 2006-07.

OVERVIEW

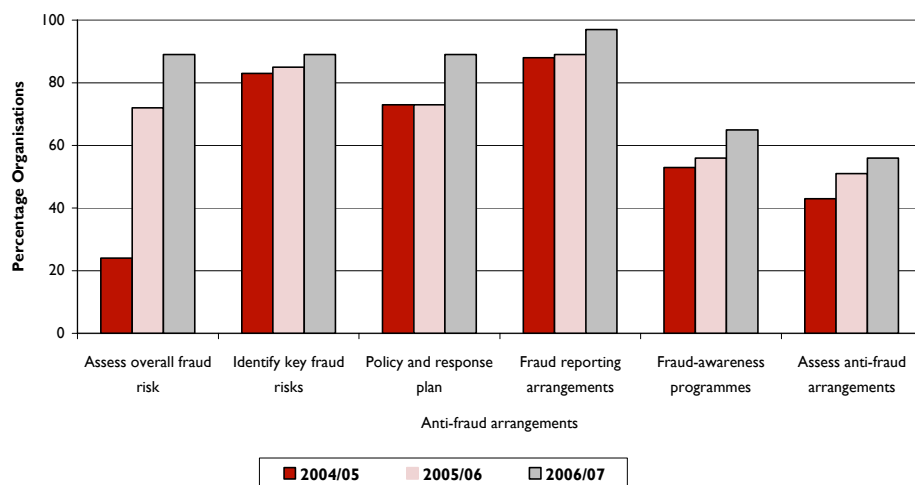
3.1 The analysis of anti-fraud questionnaires is based on information supplied by 35 Government Departments, 37 Agencies, 109 NDPBs and 63 other bodies (e.g. Special Health Trusts), 244 bodies in all. The table at [Annex A](#) is an analysis of the data supplied.

3.2 Overall, the analysis revealed that fraud is taken seriously across central Government bodies and that organisations have measures in place, or are planning to install them, proportional to the fraud risk they face, to manage fraud risk effectively and to respond to fraud when it arises. Government bodies have also carried out muchwork in recent years to improve their management of both internal and external fraud risk and [Annex E](#) provides details of measures taken by them in 2006-07.

ANTI-FRAUD QUESTIONNAIRES

3.3 A comparison of the anti-fraud questionnaire data with data supplied in the previous two years (see [figure 1](#)) shows a steady increase in the proportion of organisations that have: taken action to measure the risk of fraud that they face; raise fraud awareness; respond effectively to fraud when it arises; provide facilities for people to report their suspicions of fraud; and assess the effectiveness of their anti-fraud arrangements.

Figure 1: Comparison of anti-fraud arrangements over 3 years



3.4 The main observations from the analysis of anti-fraud management in central government bodies follow:

- Nearly all bodies (89%) assess the overall risk of fraud (some as part of their organisation's risk assessment, others by means of a separate fraud risk assessment) and identified the processes or activities most at risk of fraud. 48 bodies (20%) had assessed fraud risk as medium or high. Regular fraud risk assessments were carried out by 76% of all bodies.
- A majority of organisations (89%) had an anti-fraud policy and fraud response plan and 94% of bodies that assessed the risk of internal and/or external fraud as medium or high said that they had these or had plans to produce them. **"Managing Public Money"** states at annex 4.7 that "a fraud policy statement and a fraud response plan are two key documents that every organisation should have". All bodies provided channels for staff or members of the public to report their suspicions of fraud.
- Most organisations said that they investigated all cases of reported fraud (89%), monitored the progress of cases under investigation (82%) and took appropriate action against known fraudsters (85%). The data includes a large number of bodies where fraud is unlikely to arise and a further analysis of the data with this data removed revealed that all the remaining bodies answered 'yes' to these three questions.
- Most organisations allocated overall responsibility for fraud risk (91%) and for managing specific fraud risks (79%) to named individuals. This is a very high proportion given that around 80% of organisations considered the risk of fraud to be low.
- Although 78% of bodies said that they reviewed policies and controls following major frauds, a further analysis of the data revealed that the remaining 21% had answered 'not applicable' to this question as no fraud cases had arisen. The majority of the bodies that answered 'yes' to this question did so on the basis that they would carry out reviews if fraud arose.
- Nearly all bodies said that they employed or had access to personnel with appropriate skills and expertise to investigate fraud. It was encouraging to note that 65% of organisations said that they ran fraud awareness programmes compared to only 27% last year.
- Nearly all bodies said that they operated staff recruitment policies designed to reduce the risk of employing potential fraudsters (e.g. verifying all information supplied by potential recruits to support applications for employment and carrying out Criminal Records Bureau checks). One possible area of concern is that only 63% of organisations said that they applied higher checks to staff in sensitive posts or with access to sensitive data (although it is likely that many organisations had no such sensitive areas). Also of possible concern was that only just over half the organisations in the survey said that they applied security checks to contractors, consultants and agency staff (note: around 20% of organisations felt that such checks were not necessary as the potential for fraud was very low).
- Just over half the bodies said that they measured the effectiveness of anti-fraud arrangements (56%) or considered the risk of fraud when developing new policies and programmes (60%). The fraud-proofing of policies and

programmes is very important in the light of some policies introduced in recent years where significant fraud arose because effective anti-fraud measures were not built into them (e.g. Individual Learning Accounts, Big Lottery Fund).

- Nearly all bodies had Boards that took an active interest in their organisations' anti-fraud arrangements, received information on the progress of fraud investigations and in many cases assumed responsibility for fraud matters
- Many organisations (71%) embedded fraud risk assurance principles into contracts. Ideally all contractors/consultants should sign up to the anti-fraud policies operated by central government bodies when entering into contractual arrangements with them.
- Although only 48% of bodies said that they shared information on fraud with other bodies, this is not surprising given that only 20% of bodies had a medium or high fraud risk. However, an analysis of responses provided by those bodies with a medium or high fraud risk revealed that only 56% of them shared fraud data or intelligence. The recently completed Government Central Fraud Review made a number of recommendations about data sharing. The Government Response to the Fraud Review concluded that data sharing within and between organisations and sectors is a key factor in tackling fraud and supported the principle of greater information sharing for the purpose of detecting and preventing fraud. A good example of successful data sharing is the Audit Commission's National Fraud Initiative and more details of this can be found in **annex D**.

New or Altered Fraud-risk Management Processes

3.5 The anti-fraud questionnaire asked central Government bodies to describe details of any new or altered fraud risk management processes that were implemented in the last 3 years. The details are in **Annex E**. Some of the measures taken include:

- Individuals in the **Asset Recovery Agency** now have the management of risks, including fraud risks, inherent in their field of work embedded in their personal performance plans.
- **DfES** has introduced a tool to assist managers in assessing fraud risk.
- **Defra** has produced an interactive on-line fraud toolkit to raise fraud awareness across the Department and to provide advice about responding to fraud when it is discovered.
- **Home Office** has done a lot of work to raise staff awareness of fraud including developing an intranet site, running fraud-risk workshops and carrying out staff awareness surveys.
- The **Identity and Passport Service** has developed a risk tool which has improved both the accountability and transparency of risk identification, assessment and management.
- Work has been carried out in the **NHS Institute for Innovation** to include more robust fraud declarations in as many areas as possible (e.g. timesheets, contracts, expense claims).

- A fraud investigators' guide has been written by **Ordnance Survey** Internal Audit. They have also implemented an on-line, real-time reporting system to enable better monitoring of GPC expenditure.
- **DWP** intends to commence data-matching between its employee information and information from the Benefits system to identify and discourage employee benefit fraud.
- **HMRC** has introduced enhanced basic checking of applicants for staff vacancies to reduce the risk of employing staff who are a potential risk to the Department.

A

ANALYSIS OF ANTI-FRAUD QUESTIONNAIRES

Completed anti-fraud questionnaires were received from 35 Departments, 37 Agencies, 109 NDPBs and 63 other central Government bodies. The table below summarises the data provided. The totals recorded against each activity are where organisations operated the activity or had planned to implement it.

	Departments & Agencies		Other Bodies		Total	
	No.	% of total	No.	% of total	No.	% of total
Total number of Questionnaires completed	72		172		244	
Organisations that:						
Assessed the overall risk of fraud	69	96	149	87	218	89
Assessed the risk of internal fraud as:						
High	4	6	1	1	5	2
Medium	8	11	10	6	18	7
Low	56	78	98	57	154	63
Assessed the risk of external fraud as:						
High	6	8	7	4	13	5
Medium	12	17	16	9	28	11
Low	54	75	149	87	203	83
Identified the processes or activities most at risk of fraud	65	90	152	88	217	89
Had an anti-fraud policy and fraud-response plan	70	97	147	85	217	89
Provided clear channels reporting suspicions of fraud	72	100	165	96	237	97
Carried out regular fraud-risk assessments	60	83	125	73	185	76
Recorded and investigated all known and suspected cases	64	89	154	90	218	89
Monitored progress of all cases under investigation	64	89	135	78	199	82
Took appropriate action against known fraudsters	64	89	143	83	207	85
Allocated overall responsibility for anti-fraud strategy	69	96	152	88	221	91
Allocated responsibility for managing specific fraud risks	58	81	134	78	192	79
Reviewed policies and controls following major frauds	60	83	129	75	189	78
Used personnel with appropriate skills and expertise to investigate fraud	66	92	143	83	209	86

	Departments & Agencies		Other Bodies		Total	
	No.	% of total	No.	% of total	No.	% of total
Had effective fraud awareness programmes	55	76	103	60	158	65
Had a clear statement of commitment to ethical business behaviour	65	90	144	84	209	87
Operated an effective recruitment policy to reduce the risk of employing potential fraudsters	66	92	160	93	226	93
Checked the details and references of all potential employees	64	89	162	94	226	93
Applied higher checks to staff with access to sensitive data or in sensitive roles	55	76	98	57	153	63
Applied security checks to potential:						
Contractors	52	72	81	47	133	55
Consultants	49	68	78	46	128	53
Agency staff	53	74	88	51	141	58
Measured the effectiveness of anti-fraud arrangements	39	54	98	57	137	56
Fraud-proofed new policies and programmes	49	68	98	67	147	60
Had a Board that:						
Actively endorsed anti-fraud policies and practices	68	94	163	95	231	95
Monitored progress on major investigations	62	86	150	87	212	87
Explicitly assumed responsibility for fraud risk	62	86	122	71	184	75
Embedded fraud-risk assurance principles in contracts and commercial relationships	55	76	119	69	174	71
Shared fraud information with other bodies	28	39	90	52	118	48

B

LARGE VALUE FRAUDS PERPETRATED BY STAFF

The following summaries relate to cases with values where losses exceeded £20,000 and which were perpetrated by or involved staff (e.g. collusion with outsiders). These cases are included in the main analyses.

PAYMENT FRAUD

£1,200,000 An officer misappropriated official remittances using a variety of methods in order to divert the payments to the benefit of others (e.g. to remove an existing liability or create a false repayment situation). The fraud came to light when the department carried out routine checks into a large payment. The officer has been suspended and a full criminal investigation is being carried out with a view to prosecuting all parties to the fraud. Also, Internal Audit is carrying out a review of the system/control weaknesses that were exploited by the perpetrator of the fraud.

£400,000 An employee of a small organisation that administered a charitable fund took advantage of his position of trust to perpetrate fraud. His role allowed him to verify application forms for funding, create false applications using supporting information from genuine claims and establish false bank accounts into which payments were made.

The application forms in use contributed to the fraud (there were no inbuilt security features such as numbered forms or secure stock control and no declarations requiring signature either by applicants or professionals supporting claims). Furthermore, there were no means of verifying applicants' details and no supporting documentation, such as a passport, requested.

The perpetrator had previously been employed at another organisation from where he misappropriated £225,000 from the charitable fund. The perpetrator was prosecuted, receiving a five year custodial sentence. The fund recovered £225k from the former employer with recoveries from the perpetrator's bank account and a charge on his property resulting in a total recovery of £267,500.

A full review of the charitable fund application and payment processes was undertaken, resulting in amendments to the application forms to include declarations by applicant and counter signatory. There is now a requirement for more background information to be provided by the applicant as well as supporting documents. Additionally, the fund now has access to a central database to provide further identification checks. Additional control over the processing of applications for funding have also been introduced including, segregation of duties, random spot checks by the directors and managers and more stringent checks recruitment checks on potential employees.

£314,000 An investigation into a fraud identified by a department's internal control procedures revealed that an officer had perpetrated a number of frauds including passing details of departmental records to outsiders so that claims for bogus repayments could be made. The officer also used stolen or cloned credit cards to make payments which were subsequently reclaimed. The officer has been suspended and investigations are continuing.

£185,000 An account manager stole £185,000 over approximately two years. The fraud consisted of two elements:

- £72,000 was due to duplicate payments made, but not entered onto the accounts. Bank statements were forged to match the fake accounting record. The duplicate cheques were then cashed at a local bank for personal gain and;
- £113,000 was due to fees not being paid into the bank in full but account vouchers fraudulently amended and accounting records entered as though they were. Again bank statements were amended to hide this.

This fraud happened because of the non-application of prescribed procedures. The fraud was identified when the bank where the duplicate payments were being cashed alerted the office that the account was overdrawn. The office was not aware that the bank account had been set up and further investigation revealed the extent of the fraud. The individual was dismissed and criminal/civil recovery proceedings are underway.

£110,000 Evidence from other fraud investigations resulted in an investigation into the alleged fraudulent activities of a member of the public who was thought to be claiming benefits to which they were not entitled. A member of staff who was living with the claimant was suspected of participating in the fraud and of interfering with the investigation by intercepting a document from other fraud investigators. The member of staff was dismissed and a prosecution is pending.

£54,000 Because management checks were not routinely applied and staff were passing cases to each other for authorisation, a member of staff was able to create fictitious benefit claims in the name of family members and friends and make backdated awards into their bank accounts. Routine departmental checks detected the fraud, and subsequent investigations and prosecution resulted in a 15 month custodial sentence for the perpetrator.

£53,667 A member of staff who was in receipt of benefits from a department supplied false information about her and her spouse in order to receive more benefits. The fraud was discovered following an investigation into allegations made in an anonymous letter. A prosecution is ongoing and the department plans to take action to recover losses.

£34,004 A member of staff was found to be claiming benefit from a department whilst in employment with the department. The fraud was identified through internal control procedures. The member of staff has resigned, a prosecution is on-going and a restraining order has been placed on the perpetrator's estate until recovery action can be taken.

£32,000 An officer assisted outside accomplices to defraud a department by creating false documentation which allowed fraudulent payments to be made. The fraud came to light following a routine review of documentation. The officer was suspended from duty and legal proceedings are being considered. A review of payment processes is also to be undertaken by Internal Audit.

£32,375 An officer created a bogus company and false records resulting in him receiving payments to which he was not entitled. The fraud was discovered as a result of routine checks carried out by the department. The officer was suspended and legal proceedings are being considered.

£21,791 A staff member on temporary promotion who was frequently left unsupervised took advantage of weak controls to steal a batch of blank cheques, completing one every

week and paying them into their own bank account. The office was closing down and the proper checks were not carried out. The fraud was discovered when the perpetrator's bank alerted the department to the high level of payments received. The perpetrator was dismissed and prosecution resulted in a 12 month (suspended) prison sentence. Recovery of losses is being pursued.

TRAVEL & SUBSISTENCE AND OTHER ALLOWANCES

£126,000 Under an old HR system for processing travel claims, details of journeys made could be submitted without the dates of travel recorded. This made the checking of claims difficult and allowed the perpetrator of the fraud to submit false claims over a sustained period. The officer was suspended and subsequently dismissed. Legal action is being taken. A new system for processing travel claims has since been installed which should reduce the risk of similar frauds occurring in future. Internal Audit is to analyse the data in the old system to establish if other frauds had been perpetrated.

PAY OR ALLOWANCES PAID VIA THE PAYROLL

£87,571 Three cases in the same department involved officers taking unpaid leave and continuing to receive their salary. The cases arose because of weak controls in paper-based systems which have now been replaced by computerised systems with controls to prevent re-occurrences of this problem.

Under the paper-based system officers taking unpaid leave completed a form, setting out the period of leave applied for. This form resulted in salary payment ceasing from a given date. At the end of the period, the officer applied to re-commence work at which point the salary started again. There were no details of any completed forms on the officer's files and they continued to receive their salaries for periods of 16, 21 and 24 months respectively. It is not clear if the documentation was misplaced or never completed. The officers concerned have been asked to repay the outstanding monies. One officer has been dismissed and disciplinary measures are being considered in the other two cases.

PROCUREMENT FRAUD

£35,000 This case relates to the unauthorised purchase of IT equipment. The items were ordered through a call-off contract. On receipt of the relevant documentation a budget manager queried the provenance of the order and discovered that the individual who is thought to have placed the order had exceeded his delegated authority and may have ordered the goods for his personal benefit. The case was still under investigation at the time of reporting.

RECEIPTS FRAUD

£25,000 An employee stole £25,000 by giving unofficial receipts to applicants for services provided and by amending till records. In this way the officer was able to steal a portion of the income rather than bring it to account. The officer was dismissed and the money recovered. The police declined to prosecute as the money was repaid. As with other frauds identified, this primarily took place because of non-application of prescribed controls (i.e. unauthorised access to the till, failure to give official receipts, failure to frank application forms, failure to carry out management checks effectively) rather than gaps in the control framework. A temporary duty officer identified the fraud following the application of internal checks.

C

LARGE VALUE FRAUDS PERPETRATED BY OUTSIDERS

Members of the public or contractors perpetrated the following cases. This is not a complete list of all external fraud cases but only those that contain general lessons for other Government bodies. These cases are not included in the main analyses.

CONTRACTOR FRAUD

- £228,780** An ex-employee of an organisation claimed that staff of that company had been intentionally dismissed in order to allow them to recruit unemployed people which would allow them to claim subsidies from a department. Also, the training programme developed by the company did not meet the requirements of the contract with the department and there was some evidence to show that records had been falsified to give the impression that customers had received support when they had not. The service provided was significantly below the set standard and failed to allow the customers to benefit from the support and time designated to them in the contract.
- £194,195** A contractor, engaged in training members of the public, deliberately progressed large numbers of course participants onto an advanced stage of courses before they were ready for that stage. The contractor had not agreed to repay all losses at the time of reporting and the case was being considered by the Department's solicitors.
- £106,000** The case concerns an employee of a major contractor who, over a period of six years, used the contractor's (and before that, the previous contractor's) corporate credit card to purchase foreign currency. The employee was a personal assistant to a senior manager. Despite there being no requirement for foreign currency, the individual managed to avoid detection by arranging for the currency to be collected by her in person only, and printing false invoices for rail tickets. The credit card statements signed off by the manager listed the travel agent used for the transactions only. A considerable number of legitimate journeys to both London and Manchester are regularly booked for staff.
- The fraud was detected when the individual was on leave and the travel agency sent the currency to the contractor. Senior managers were asked to sign for the safe delivery of packets of euros they had not ordered. Once alerted to this, the Managing Director called the travel agent who explained that the currency had been requested by the PA and that it was a regular transaction. The contractor's internal security team has conducted a formal investigation and the individual has been sacked. The costs that were incurred (£106,000) have been repaid by the contractor in full. The Police have now interviewed the individual and who may be prosecuted.
- £83,790** The premises of a contractor providing training services on behalf of a department to members of the public was raided by the police following an allegation that test passes were being sold to candidates. A number of files have been removed and so far there is evidence to support an allegation of fraudulent activity including false records and forged signatures which may have been used to support claims for funding from the department. The contract with the supplier has been cancelled and recovery action is planned. An external audit has been commissioned to establish the weaknesses that allowed the fraud to occur and to make recommendations about reducing the risk of similar frauds occurring in future.

- £73,000** A whistle blowing complaint from a former employee of a contractor that provided educational services on behalf of a department to members of the public alleged falsification of records in support of funding claimed. An examination of funding claims by the department revealed a number of indicators of fraud including possible fraudulent amendments and forged signatures. The police are investigating the case. The department has carried out a major review of control processes and has installed more robust audit processes, regional funding and established a national networking process to increase the chance of problems being spotted early and dealt with quickly.
- £33,229** A Department's inspectors highlighted a contractor's persistent failure to retain acceptable evidence in support of their Job Outcome Fees (JOF). Sampling identified 53 outcomes which did not meet the JOF criteria and enquiries revealed that the corresponding details of the participants' employment had not been independently endorsed. Contractor staff had entered information on stencils (which have to be completed by the employer) and where, alternately, the participants' endorsements had been sought, the required additional evidence had not been obtained. Although outcome fees totalling £33,229 were found to be invalidated, only £10,152 was recovered from the contractor who successfully argued that an alternative interpretation could reasonably be inferred from Departmental guidance for most of the period of overpayment.
- £21,294** A provider claimed and received funding from a department relating to the provision of services to departmental customers which were not provided. The overpayment was identified by the departments control procedures and action has been taken to recover the losses.

EXTERNAL FRAUD

- £1,080,124**
£57,953 Two cases were reported involving the theft of money by local authority employees responsible for managing the finances of those with reduced mental capacity. The larger value case had been perpetrated over a 9 year period and was discovered through money laundering checks carried out by a bank. The fraudster received 3 years imprisonment. The second case involved systematic fraud over 13 months and was discovered during a period of absence of the employee responsible. Both cases involved taking advantage of fundamental weaknesses in checks and controls and an absence of fraud awareness among those responsible for supervision. The fraudster was sentenced to 12 months imprisonment. The losses totals include estimates of interest lost over the periods in which the frauds were perpetrated.
- £127,683** This case involved the theft of 920 blank cheques from a safe at a regional office. Poor security at the office allowed the theft to take place and a police investigation failed to identify a perpetrator. Improved security arrangements have been implemented at the office.
- £112,419** A customer was awarded 'Travel to Work' funding for taxi journeys between their home and London where they claimed to be undertaking work with a wide range of organisations for their employer. No change in taxi fares occurred over the following 3 years and concerns around the authenticity of receipts submitted prompted an investigation. The findings suggested that the customer had deliberately misrepresented the status of their position in the company, the extent/nature of their work and the level/means of travel involved. They were found to be the proprietor of the business and the person to whom they attributed ownership was their spouse, using a previous name. The customer failed to produce any evidence of business activity

consistent with the terms of the award and none of the taxi drivers/operators from the receipts could be located. The customer and their spouse declined the opportunity to explain the irregularities at formal interview so all claims were deemed invalid due to the false premise of the original application. Action is being taken by the department to recover the losses and this is one of several cases used to justify recommendations to the Department's National Team around the verification of evidence supporting travel cost claims.

- £38,021** As a result of concerns expressed by a customer's employer, it was discovered that the customer had been claiming benefit to which they were not entitled. The fraud involved the submission of false evidence which included forged employer declarations to support claims. No action has been taken against the individual on the grounds of ill health.
- £22,322** During a routine check with an employer it was discovered that a member of the public who submitted regular claims to a department for taxi journeys to and from work did, in fact, drive himself. Claims for payment were supported by forged taxi receipts. The perpetrator was prosecuted and recovery action is being considered.
- £20,622** A department's checking procedures identified a client who was claiming funds for a support worker to drive him to and from work when in fact no such support worker existed and the client was living close to his workplace. Action is being taken to recover the loss.
- No Loss** The police reported that a number of cheques for fees due to a department had been intercepted and the details fraudulently changed. The cheque fee amount of £120 had been changed to such amounts as £34,120, £230,120, £38,120, and £24,500. The police successfully prosecuted one person for attempting to obtain property by deception who received 15 months imprisonment. An internal investigation revealed no evidence that departmental employees were involved in the frauds.
- No Loss** An attempt was made to divert two compensation claims totalling £52,750 to false bank accounts established by the perpetrators. The nature of the fraud suggested that the perpetrators had some knowledge of the organisation's procedures and it appeared that mail had been intercepted and some substitution of documents had taken place. Internal audit carried out an internal investigation and the police pursued enquiries into the alleged perpetrators who were known to them. It is unlikely that the police investigation will result in any action against the suspected perpetrators and in the meantime internal procedures have been strengthened.

This section covers fraud-related issues including the Government Fraud Review; services available from the NHS Counter Fraud and Security Management Service; the new Ministry of Justice; a variation on Advance Fee Fraud; EU fraud; relevant PAC Reports; and the Audit Commission's forthcoming datamatching exercise.

GOVERNMENT FRAUD REVIEW

D.1 In October 2005 the Attorney General and the Chief Secretary to the Treasury commissioned the first holistic review of Fraud in England and Wales. The interdepartmental team conducting the review was drawn from the Attorney General's office, HM Treasury, Ministry of Justice (then DCA), Serious Fraud Office, Crown Prosecution Service and the City of London Police; but a great many more departments were represented on the Steering Group that the Attorney General set up to oversee the work. The review was asked to consider:

- The scale of the (fraud) problem;
- The appropriate role for Government in dealing with fraud;
- How resources could be spent to maximise value for money in this.

D.2 The Report was published in July 2006 and contained 62 recommendations. Following public consultations the Government response was published on March 15th 2007 (www.attorneygeneral.gov.uk).

D.3 Seven key areas were identified for implementation. Seven public/private sector working groups have been set up, to provide detailed budgets and business plans on the following:

- National Fraud Strategic Authority;
- Measurement Unit;
- National Fraud Reporting Centre;
- National Lead (Police) Force;
- Crown Court Powers;
- Financial Court;
- Framework for Plea Negotiations.

D.4 This work is being overseen by a high level Programme Board, chaired by Jenny Rowe, Director of Policy at the Attorney General's Office. The Board aims to provide implementation plans for the approval of Ministers early in 2008.

D.5 This policy initiative is linked to ongoing work in the Home Office and the Ministry of Justice. The Office for Criminal Justice Reform is closely involved. It aims to bring together public and private sector anti-fraud efforts into a co-ordinated national strategy that addresses both upstream fraud prevention and public awareness activity and downstream savings on detection, investigation and trial costs. It is anticipated that

the National Fraud Strategic Authority will be Government led, but established as a full public/private partnership reporting to a governing body representing all major public and private sector stakeholders.

D.6 Some of the recommendations are for longer term projects in the criminal justice area; for example, extended Crown Court powers which will require primary legislation. It is however intended that the National Fraud Strategic Authority and its Measurement Unit will be in place in 2008 and that the Reporting Centre and Lead Force arrangements will follow swiftly afterwards

D.7 The Fraud Review public consultations attracted significant interest, particularly from professional bodies, corporate victims of fraud and anti fraud organisations such as the BBA, ABI and CIFAS. Many are contributing already to the working groups and, additionally, a Stakeholder Group has been formed to provide a further pool of expertise and skills for the National Fraud Strategic Authority and the National Fraud Reporting Centre. Although the Review originally excluded revenue and benefit fraud, its recommendations extended to all forms of fraud. The DWP, HMRC, DofH, DTI, OFT, FSA, NAO, the Charity Commission and the Audit Commission are now amongst the departments and agencies that are actively involved in the working groups alongside the Criminal Justice Departments and HM Treasury.

D.8 Progress reports on the ongoing Fraud Review work, together with the original Review and the Government Response, can be found on www.attorneygeneral.gov.uk. Further information on the work of the Fraud Review can be obtained from the team administrator at the Attorney General's Office, 20 Victoria Street London SW1H 0NE; tel: 0207 271 2448.

THE FRAUD ACT 2006

D.9 The UK Fraud Act 2006 came into force on 15 January 2007. 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).

D.10 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 a CV in order to secure a job).

D.11 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 omission rather than by an act or acts.

D.12 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.

COUNTER FRAUD AND SECURITY MANAGEMENT SERVICE (NHS CFSMS)

D.13 The Counter Fraud and Security Management Service is a division of the NHS Business Services Authority and has responsibility for all policy and operational matters relating to the prevention, detection and investigation of fraud and corruption, and the management of security in the NHS. They offer a number of counter-fraud services to other bodies including training, consultancy, documentation, risk measurement and research.

For more detailed information about services available please contact the NHS CFSMS by email on comdev@cfsms.nhs.uk or by telephone on **0207 895 4777** or visit their website: <http://www.cfsms.nhs.uk/commercial/index.html>

MINISTRY OF JUSTICE

D.14 On 9 May 2007, the responsibilities of the Department for Constitutional Affairs were transferred to the Ministry of Justice which is responsible for the courts, prisons, probation, criminal law and sentencing. More details about the new department can be found on its website: <http://www.justice.gov.uk/>

ADVANCE FEE FRAUD

D.15 The Metropolitan Police have issued the following fraud alert:

- Emails and letters are currently circulating that purport to be from the EU Humanitarian Grant, Special EU Programmes Body. We have been advised by the EU that no such body exists within the EU.
- The emails / letters contain wording which indicate these are precursors to 419 advance fee frauds. The emails will be readily identifiable as they do not originate from a genuine EU email address, bearing sender addresses such as notify@weboffice.com. In addition both the emails and letters provide platform numbers as telephone contact details, which start 0701, 0702, 0703 or 0704. The EU would not use such types of phone numbers.
- Do not respond to these emails / letters in any form as they will result in a request to provide fees up front under various excuses to cover various payments. Under no circumstances send any money in response to these mailings.

FRAUD AGAINST THE EU BUDGET

D.16 The annual European Community budget for 2007, funded by contributions from the 27 Member States, comprises around €115 billion (£78 billion¹). Around 80% of this total is managed directly by Member States on behalf of the European Commission. This directly-managed money includes Agriculture funds (Common Agricultural Policy, Fisheries and Rural Development spending) and the Structural and Cohesion Funds (which aim to finance investment in education and training, innovation and research, transport and energy, and support for regional and local development). Each Member

¹ Converted at the exchange rate on 29 December 2006: £1 = €1.489203

State receives an allocation of these funds. In the 2006-7 financial year, the United Kingdom received an estimated:

- £3,312 million from the Agriculture Guarantee fund (CAP)
- £1,829 million the Structural Funds; and
- £23 million in other receipts from the Community budget.

D.17 In the UK, these funds are managed by several Government Departments, Regional Development Authorities, regional Government Offices and the devolved administrations of Scotland, Wales and Northern Ireland. The work of managing the funds involves:

- checking and paying claims from farmers for the Single Farm Payment scheme
- approving applications to run projects co-financed by the Structural Funds (the rest of the finance comes from other national sources)
- checking eligibility and compliance with many and detailed Regulations
- making payments under the Structural Funds and Agriculture Regulations.

D.18 Managing EU funds is considered to be a high-risk area because of:

- the number of levels involved – separate managing, certifying and paying authorities, beneficiaries, recipients etc
- the complexity of the regulations and the impossibility of checking every claim against complex eligibility criteria.

D.19 Managing EU revenue is also a complex area. The Community budget is funded by Member States contributions from customs duties, including those on agricultural products, and sugar levies (these are referred to as Traditional Own Resources), VAT-based contributions and GNI-based contributions. Missing trader or “carousel” fraud on VAT is a high risk area.

D.20 But while there is a relatively high risk of fraud overall, in fact the amounts of detected and reported fraud are relatively low. The European Anti-Fraud Office (OLAF) has the main responsibility for investigating suspected frauds reported by Member States. In 2006 (the latest year for which figures have been published), OLAF estimates that around €29.8 million (£20.3 million²) fraud was committed against the Agriculture budget (0.06% of the total budget for Agriculture) and around €157.6 million (£107.4 million) against the Structural Funds budget (0.41% of the Structural Funds budget). On the revenue side, OLAF reveals that €134.4 (£91.6 million) fraud was reported against traditional own resources, around 0.94% of the total from this source of revenue for 2006.

D.21 The UK reported the following frauds against the EU budget in 2006-7 to the European Commission. These cases are included in the OLAF figures given in the previous paragraph:

- **Revenue:** One case, involving Customs duties of £539,459;

² Euro figures as published in the 2006 “Fight against Fraud” report. This, and all remaining sterling figures in this paragraph, has been converted from euros at the annual average rate for 2006: £1 = €1.4669.

- **Agriculture:** 6 cases, total amount involved from the Community budget of £123,487;
- **Structural Funds:** 9 cases, total amount involved from the Community budget of £1,320,049;

D.22 Details of some of the cases reported include:

- The Rural Payments Agency (RPA) reported one case related to the Processing and Marketing Grant Scheme. The total amount involved was £169,361.41 (funded 50/50 by national and Community budgets - £84,680 from the Community budget) with an additional 10% penalty of £16,936.14. The claimant incurred expenditure before the grant was agreed although he had signed a declaration stating that such expenditure would be ineligible. He then deliberately falsified documents to meet the criteria of the scheme rules. This was identified during a Scrutiny Visit by the RPA's Counter Fraud and Compliance Unit.
- Two cases reported from the Structural Funds sector by the Department for Business, Enterprise and Regulatory Reform involved the same individual, whose business has gone into liquidation and who is known to have left the country. The two cases involved a total amount of £82,268 paid from the Community budget

D.23 Information sources on the subject of EU fraud include the following:

- The European Anti-Fraud Office (OLAF) www.ec.europa.eu/anti_fraud/index_en.html
- Eurojust www.eurojust.europa.eu
- European Commission www.europa.eu/index_en.htm
- European Community Finances: Statement on the 2007 EC Budget and measures to counter fraud and financial mismanagement (published by HM Treasury) www.hm-treasury.gov.uk/media/2/8/ecbudget220507a.pdf
- Financial Management in the European Union (annual report from the National Audit Office) www.nao.org.uk/publications/nao_reports/06-07/0607401.pdf

PAC REPORTS

D.24 HC765 (27 April 06): Tackling the Complexity of the Benefits System - this Report claims that a consequence of the complexity of the benefits system is a high level of fraud and error. The DWP recognise the problem and has taken a number of steps to reduce the level of fraud and error, and intends giving greater priority to tackling complexity

D.25 HC782 (25 April 06): Inland Revenue Standard Report: New Tax Credits - this Report relates to fraud in the Tax Credits system, recommending that the Department, when designing similar schemes in future, should assess the level fraud and error and their ability to identify and manage it.

D.26 HC874 (22 June 06): HM Customs and Excise Standard Report 2004-05 - this report provides an update on how HMCE is dealing with the problems of tobacco smuggling and VAT fraud.

D.27 HC918 (18 May 06): Governance Issues in the Department of Enterprise, Trade and Investment's Former Local Enterprise Unit - this case involves conflict of interest and impropriety in which the Department failed to ensure that the basic principles of proper conduct of public services were observed in one of its NDPBs.

OPPORTUNITY TO PARTICIPATE IN AUDIT COMMISSION DATA MATCHING EXERCISE

D.28 The Audit Commission's National Fraud Initiative (NFI) has run every two years since 1998 and is firmly established as the United Kingdom's premier public sector fraud detection exercise. It uses advanced data matching techniques to tackle a broad range of fraud risks faced by the public sector such as widespread non-declaration of income by benefit claimants, council tenancy and right to buy abuse and employment fraud by failed asylum seekers and UK visa overstayers.

D.29 The value of fraud and overpayments detected by almost 1,300 public bodies taking part in the NFI 2004/05 exceeds £111 million, an increase of 33 per cent on 2002/03.

D.30 Despite the successes of NFI, there is scope to develop it further and in February 2005, an opportunity arose to demonstrate the NFI to the government's Wide Ranging Review of Fraud. The Review Team saw the potential of NFI to provide some quick and low-cost wins for central government and agreed to support the Commission's request for additional powers if it could be demonstrated that these could be of wider benefit to the public purse.

D.31 These additional powers now form part of the Serious Crime Bill that was introduced in the House of Lords on 16 January 2006 and will insert additional provisions into the Audit Commission Act 1998 (ACA 1998).

D.32 Bodies other than those that have a mandatory requirement to provide data for NFI, including those outside England and Wales, can then volunteer to participate by providing data to the Commission. This means that Government Departments and Agencies will also be able to participate in future NFI exercises and can immediately benefit from some of the existing suite of data matches (**Table 1**). The Commission plan to hold workshops with Government Departments to establish if there are any other risks that NFI could address through data matching.

Table 1 – existing areas available immediately

Data	Examples of issue identified
Payroll	Employees who are absent through sickness but are found to be working elsewhere. Employees with no recourse to public funds but who are claiming benefits.
Failed asylum and UK visas	Employees with no entitlement to reside in the UK or entitlement to work
Deferred Pensions	The pension scheme has not been notified of the death of the pensioner so the widow(er)'s pension payments are possibly not being made correctly to dependents.
Trade creditors (i.e. suppliers of services)	Duplicate payments of invoices and governance issues such as undeclared interests

D.33 The Commission has a Code of Data Matching Practice which bodies providing data for the exercises must have regard to. The code sets out the governance arrangements, security standards and requirements for fair processing that must be adhered to in carrying out data matching exercises, and will assist in ensuring full compliance with the Data Protection Act. The current Code of Data Matching Practice binds the Commission to conduct data matching only in areas where there is existing evidence of fraud, to ensure the exercise is targeted.

D.34 Some of the other areas that the Commission plans to include in the NFI are:-

- Child protection (i.e. matching to the sex offenders register and the Education Act, section 142, Teaching prohibition list);
- Non-fraud areas - in particular any type of arrears left by absconders for example local authority arrears such as council tax, rent, as well as Magistrates Courts fines;
- Data from The Council for Mortgage Lenders will assist with owner occupier and landlord housing benefit fraud;
- Housing Associations – Local authorities are continuing to sell off housing stocks to external landlords taking social housing tenancy data outside the current remit of NFI. Therefore, this is a particularly important data source to ensure 100% of housing stock is available to assist with tenancy fraud in a more comprehensive manner. Housing Associations could benefit from most of the existing suite of data matches for example, trade creditors, tenants and payroll matches;
- Cross border matching of data from participants in England, Scotland and Northern Ireland;
- Identity fraud - a new approach is planned to identify fraudulent identities;
- For more information please visit the NFI web page www.audit-commission.gov.uk/nfi.

E

ANTI-FRAUD INITIATIVES

Departments and sponsored bodies have been very active in developing processes and controls to reduce the risk of fraud in their organisations and below are some examples of actions taken.

ASSETS RECOVERY AGENCY

E.1 Individual team members now have the risks inherent in their field of work, including risks of fraud where appropriate, embedded in their Personal Performance Plans. The impact is hard to gauge but the approach serves to make everyone risk aware and makes it clear that they are all contributors to risk management.

MINISTRY OF DEFENCE

E.2 Recognising that existing procedures for the reporting of suspicions were haphazard and suffering from non-compliance, the department created the Defence Irregularity Reporting Cell as a 'one stop shop' for recording suspicions, allocating these to the appropriate investigative authorities and monitoring the progress of investigation, outcomes etc. The result has been a marked increase in the volume of reported suspicions and greater oversight of investigative processes.

DEPARTMENT FOR CHILDREN, SCHOOLS AND FAMILIES (DCSF)

Department

E.3 The Department has reviewed its approach to fraud management with partner organisations and introduced a management tool to assist managers to assess the risk of fraud. There has been a great deal of activity to raise the profile of fraud risk management and prevention strategies.

Department for Innovation, Universities and Skills (DIUS)

E.4 The Department has undertaken specific work in the area of Student Loans and has tightened application processes which should lead to improved fraud prevention. Examples of recent measures taken by the Students Loan Company include:

- Agreement reached with Audit Commission that the Students Loan Company will participate in datashare in 07/08.
- The Student Loans Company no longer accepts birth certificates alone as proof of identity. Also, applicants without a valid National Insurance number will not receive funding.
- Agreement has been reached that local authorities and higher education institutions keep the Student Loans Company informed when applications for funding have been stopped.

- The Student Loans Company will regularly review and revise its anti-fraud guidance for Local Authorities and Higher Education Institutions.
- The new fraud policy has been approved by the Audit Committee and work on raising anti-fraud awareness is planned.
- Appropriate for a?? are being targeted to raise anti-fraud awareness in Local Authorities and Higher Education Institutions.
- Steps are being taken to improve the process of informing the Student Loans Company when students withdraw from courses. A non-completers audit is to be carried out later in the year.
- A sound process for reporting and investigating fraud cases has been established and meetings with the police have helped to agree a robust protocol for prosecuting known fraudsters.

DEPARTMENT FOR ENVIRONMENT, FOOD AND RURAL AFFAIRS

E.5 An enhanced anti-fraud strategy, response plan and generic departmental fraud risk assessment has been rolled out across the Department and awareness education is continuing. The education and raising awareness of fraud has included the introduction of an interactive (on-line) Fraud Toolkit to help understand aspects of fraud and how to deal with any suspected fraud. The Toolkit has the potential to be used as a best practice guide across the Defra Network; this will be promoted in the coming year. The Toolkit site provides advice, guidance and tools for Defra staff who need to know more about fraud, how to identify it and what to do if they have any concerns.

E.6 The toolkit is divided into the following sections:

- Frequently Asked questions - General advice and guidance in dealing with fraud.
- Identifying Fraud - Some examples of fraudulent activities.
- Responding to Fraud - Advice and guidance on what to do if you suspect a fraud against the department.
- Tools & Guidance - General tools and information to assist in prevention of, raising awareness of and dealing with fraud.
- Need to speak to someone? - Who to contact for further advice or guidance.

E.7 In addition to the activities described above, fraud awareness was introduced in the Director General Statement of Internal Control workshops this year to increase exposure and raise fraud awareness. However, given the overall low internal fraud assessment it will be some time before the effects of the enhanced fraud awareness material will become embedded in the day to day work

HOME OFFICE

E.8 The main initiatives over the past year have focused on:

- Raising fraud awareness within the Department via briefings, various articles featuring matters such as fraud issues, Civil Service Code, the work of the Anti-fraud and Investigation Team (AFIT);
- Staff awareness surveys;

- Developing the AFIT intranet site (which now provides access to relevant policies and guidance for staff and management);
- Running fraud risk workshops (10 workshops held);
- Publicity by the Permanent Secretary for the new Civil Service Code on the intranet and in the in-house magazine;
- Providing updates for management, auditors and investigation teams on the Fraud Act 2006 and anticipated provisions relating to data matching in the Serious Crime Bill 2006-07
- Providing targeted briefings for management covering such things as key messages from the Treasury's Annual Fraud Report and risk surveys on managing fraud risks.

E.9 The main benefits accruing from the above initiatives have been the raising of the confidence levels of staff in the reporting of fraud and irregularity and in raising management's awareness of the exposure to the generic risks of fraud and irregularity. The Fraud Risks Workshops have in particular generated wide-ranging issues for follow-up by management.

E.10 Looking forward to 2007-08, the internal audit function is giving greater emphasis to audits that relate to the corporate processes of accounting, procurement, human resource management (including payroll) and areas of financial risk. They are also doubling the amount of compliance audit work undertaken. The compliance programme will look at basic finance, procurement, human resources and grant processes. By reminding everyone about their responsibilities relating to the operation of key processes they aim to incrementally improve the level of compliance and thereby promote a culture of accountability, propriety and regularity.

IDENTITY AND PASSPORT SERVICE (IPS)

E.11 The Agency has moved towards a regime of facilitated control risk self assessment workshops. A network of risk co-ordinators in regional offices and HQ business units has been established to raise the profile of 'risk' as a driver for achieving assigned responsibilities.

E.12 The agency is also actively seeking to improve the assurance regime via the current year's compliance visits to provide further assurance that relevant processes and procedures are being and regularly reviewed to ensure consistency at diverse locations.

E.13 A new risk tool was rolled out between September 2006 and March 2007 which has improved both the accountability and transparency of risk identification, assessment and management.

E.14 The IPS Corporate and Business Plan 2006-2016 provides full details of their fraud risk management and counter fraud initiatives.

NHS INSTITUTE FOR INNOVATION

E.15 Work has continued to include more robust counter fraud declarations in as many areas as possible, from a fraud prevention / deterrent perspective including: timesheets, contracts, expense claims, ordering controls and expenditure controls. Also, an annual staff declaration has been introduced to declare such issues as potential conflicts of interest, which HR have stated has already provided relevant information from staff to ensure possible conflicts are resolved.

ORDNANCE SURVEY

E.16 A Fraud Investigator's Guide has been written and published by Internal Audit, and approved by the Audit Committee to guide staff through the process if a fraud is suspected or reported. Also a system called D.Cal had been implemented which allows online, real-time reporting of GPC card purchases enabling line managers to view what is being spent. This also allows more timely reporting and more visibility of expenditure at a detailed level minimising the opportunity for fraudulent purchases.

HER MAJESTY'S PRISON SERVICE

E.17 Unannounced visits focussing on areas of higher risk but low audit/management coverage have been introduced. Computer interrogation software (CAATs) will be used to identify high-risk areas and changes in trends for inclusion in visits programmes.

HER MAJESTY'S REVENUE AND CUSTOMS (HMRC)

E.18 The introduction of SIGCom, inspection of HMRC by HM Inspector of Constabulary (HMIC) has improved the structure and high-level management of the risk of fraud. Enhanced basic checking of recruitment has improved the integrity of the recruitment process and identified individuals who were considered to be a potential risk to the department.

E.19 The Intelligence Function within Internal Governance, including Financial and Analytical support, has been enhanced to identify and prioritise risks from internal fraud to business areas in line with the National Intelligence Model. Linked in with Professional standard departments within Police and SOCA, this allows cross-pollination of current and developing threats from Organised Criminal Gangs.

DEPARTMENT FOR TRANSPORT (DFT)

Department

E.20 The Department, in conjunction with the Audit Commission, carried out an online fraud awareness survey and followed up with a number of workshop sessions with staff. The objective of the fraud awareness survey and workshop was to enable senior officers in the Department to:

- clarify the anti-fraud and corruption arrangements at DFT;
- increase awareness of anti-fraud and corruption arrangements at DFT; and
- identify areas where further improvements can be made to anti-fraud and corruption arrangements.

The workshop element also included:

- presentations on the changing nature of fraud and the importance of a robust ethical governance environment;
- a questionnaire feedback to assess staff perception about the anti-fraud and corruption approaches within DfT corporately and within each directorate;
- a syndicate exercise and feedback session where attendees discussed the practicalities of introducing an anti-fraud and corruption culture; and
- consideration of ethical scenarios as they impact on DfT staff.

The results have enabled the Department to benchmark itself against other public sector bodies and to identify areas of concerns and improvement. The information collected is currently being used to further develop and improve the fraud risk and corporate governance arrangements.

Highways Agency

E.21 The appointment of a Fraud Management Adviser to act as a focal point for all fraud matters is now well embedded and all investigations are routed through him. The Group Financial Director has overall responsibility for fraud matters and periodically chairs the Highways Agency Fraud Committee with appropriate Directors to review individual investigations and general policies.

Driving Standards Agency

E.22 All fraud processes are undergoing extensive review - new anti-fraud initiatives currently being progressed revolve around a new memorandum of understanding with the association of Chief Police Officers for information sharing and closer working on ID fraud and illegal driving instruction. Scoping work is being undertaken around fitting CCTVs in practical driving test centres to assist with the identification and investigation of ID fraud.

Other DfT Bodies

E.23 The **British Rail Board (Residuary)** (BRBR) has moved to electronic funds transfer for settlement of ill health claims in excess of £20k; **British Transport Police** has introduced robust systems and processes over procurement activities which aim to facilitate the force's spending under a controlled and informative environment; **Trinity House** has implemented a new policy on security vetting for sensitive posts; the vehicle Certification Agency has implemented new controls to strengthen fraud and risk management.

DEPARTMENT FOR WORK AND PENSIONS (DWP)

E.24 The Department treats staff-perpetrated fraud very seriously, whilst recognising that only a relatively tiny minority of its employees commit workplace fraud and other related wrongdoing. During the past year the Department's Risk Assurance Division (which carries out staff investigations on behalf of management) has:

- Further developed a programme of intelligence-led work which is aimed at proactively uncovering frauds (based on a threat assessment) which have not already been identified and reported through routine methods;

- Published a leaflet to all staff supporting the Department's anti-fraud policy, and encouraging staff whistleblowing;
- Provided a significant number of awareness presentations to senior managers and downwards, covering the risk of staff fraud, and how to mitigate these risks;
- Worked closely with, or supported other parts of the Department (eg Human Resources, Internal Audit, the Departmental Security Officer, and Managers);
- Introduced a new management information system which improves the consistency of overall case management;
- Carried out an investigation into the circumstances which led to a major fraud on the tax-credit system in December 2005 using DWP employee data, and helped the Department make improvements in the secure handling of employee data;
- At the end of the year announced its intention to commence data-matching between its information held about employees (e.g. on the payroll) and information from the benefit systems which the Department is responsible for managing following consulting the Departmental Trade Unions (the first exercise of this type was conducted in April 2007). These processes help to identify and discourage employee fraud of the benefit systems;
- Introduced from April 2007, a new role of 'Prevention and Deterrence Manager'. This post will, through close engagement, further improve general Departmental managers' understanding of the threats from employee fraud and how to manage these threats.

OTHER BODIES

E.25 Many other bodies established new or revised existing anti-fraud arrangements. Examples of activities included:

- Developing or revising anti-fraud policies, fraud response plans and whistleblowing arrangements. Work also included the establishment of processes for monitoring adherence to anti-fraud policies (e.g. by internal audit);
- Developing or updating fraud risk management processes including creating or updating fraud-risk registers. In some cases this included the development of processes to ensure identified fraud risks were actively managed. One organisation developed a web-based register for the recording and management of fraud risk;
- Introducing processes to raise staff awareness of fraud (e.g. part of induction training for new staff, workshops, staff newsletters, anti-fraud guidance, fraud alerts on Intranet). A small number of bodies had also provided staff with specialist counter-fraud training;
- Clarifying responsibilities for managing fraud risk such as establishing a Fraud Liaison Officer and creating an anti-fraud unit;
- Matching fraud data with data held by other organisations and/or becoming members of cross organisational anti-fraud groups designed to share information on fraud and discuss ways to combat fraud;

-
- Implementing stronger internal control over tendering, cash handling, identity theft, staff recruitment, expense claims, setting up suppliers and contractor performance;
 - Introducing new measures to reduce the risk of cheque fraud such as moving as many creditors as possible onto electronic payments such as BACS, retaining completed cheques in Finance until they are posted and posting in street post boxes rather than have them collected by the Post Office;
 - Strengthening recruitment procedures and employee vetting arrangements (e.g. CRB clearance checks);
 - Improving security surveillance such as installing CCTV networks;
 - Introducing better vetting of visitors and contractors.

ISBN 978-1-84532-363-5



9 781845 323639 >