National Fraud Initiative in Scotland

Code of data matching practice

Prepared by Audit Scotland

July 2006

AUDIT SCOTLAND

Audit Scotland is a statutory body set up in April 2000 under the Public Finance and Accountability (Scotland) Act 2000. It provides services to the Auditor General for Scotland and the Accounts Commission. Together they ensure that the Scottish Executive and public sector bodies in Scotland are held to account for the proper, efficient and effective use of public funds.

Contents

Foreword

Over the last decade the National Fraud Initiative (NFI) has successfully detected fraud and overpayments and related forward savings of more than £300 million across the UK. Scotland's share of this total is around £23 million. This has enabled public money to be directed back towards the public services for which it was intended. Active detection and prosecution of fraudsters is a vital deterrent to others contemplating defrauding the public purse.

In addition to these benefits, these data matching exercises are an efficient tool for assisting auditors to assess the financial control and value for money arrangements put in place by audited bodies. Further, as a consequence of investigating matches that reveal overpayments, underpayments and other inaccuracies in records, the accounts of audited bodies can be corrected.

Audit Scotland and the Audit Commission's NFI appointed auditor (with whose assistance NFI takes place in Scotland) encourage all those participating in the NFI, both auditors and bodies supplying data for matching, to comply with best practice and the law when sharing and matching personal data. To that end, Audit Scotland has issued this Code for application by auditors and audited bodies in Scotland.

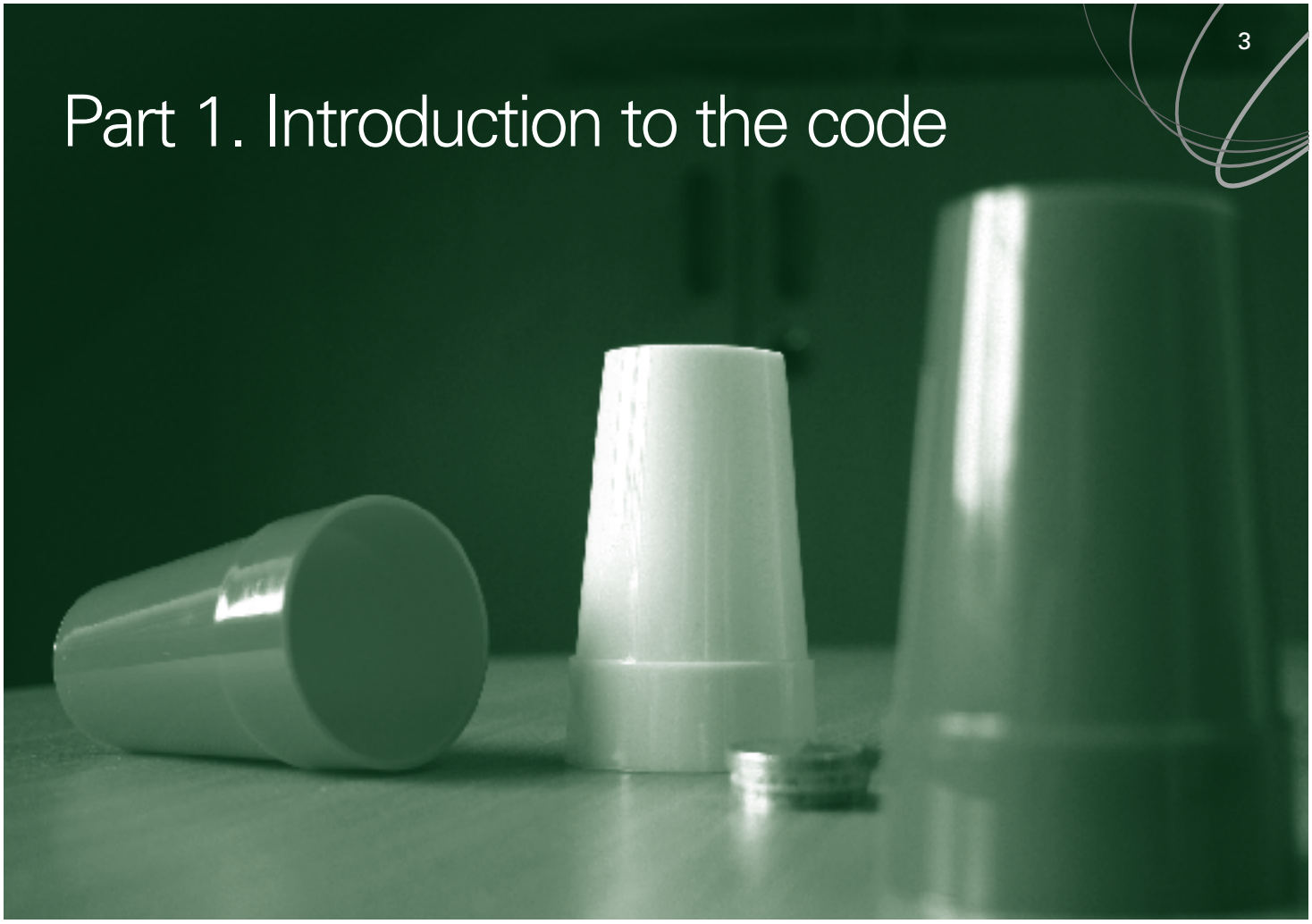
This Code sets out the principles and practices that should be adopted to ensure appropriate safeguards are built into the NFI in Scotland. The matching process must be proportionate so that fraud is prevented and detected, while law-abiding citizens' privacy and rights are respected and protected. A key aspect of the Code is to provide good practice examples of how individuals should be informed of the checks carried out.

This Code applies in relation to the statutory audit of bodies in Scotland to which the Accounts Commission and the Auditor General appoint auditors. The Audit Commission has adopted a similar Code.

NFI is a very successful example of joined-up working between our respective organisations. Audit Scotland will seek to develop the NFI in Scotland in parallel with UK developments and, wherever possible, by extending the exercise to a wider range of bodies in Scotland.

Robert W Black
Auditor General for Scotland
July 2006

Part 1. Introduction to the code



1.1 The Accounts Commission

1.1.1 The Accounts Commission (the Commission) is responsible for appointing auditors to local government bodies in Scotland. The Local Government (Scotland) Act 1973 (the 1973 Act) requires the Commission to appoint auditors to each audited body.

1.2 The Auditor General for Scotland

1.2.1 The Auditor General for Scotland (AGS) is responsible for deciding who should audit most of the other public bodies in Scotland, including National Health Service bodies, the Scottish Executive, Executive Agencies and Non-Departmental Public Bodies in Scotland. The Public Finance and Accountability (Scotland) Act 2000 (the 2000 Act), in effect, requires the AGS to appoint auditors to each audited body outside the local government sector.

1.3 Audit Scotland

1.3.1 Audit Scotland is a statutory body set up under the 2000 Act to provide services to the AGS and the Commission. In practice Audit Scotland employs the staff and incurs the expenditure required to support their functions. Except where the distinct parties require to be identified (eg, in relation to statutory powers and duties), and reflecting the practicalities of this relationship, this Code refers mainly to Audit Scotland.

1.4 Auditors for the purpose of the National Fraud Initiative

1.4.1 To minimise costs and for practical reasons, appointed auditors of local authorities are assisted for the purpose of the National Fraud Initiative in Scotland (NFI) by designated officers in Audit Scotland and by the Audit Commission's NFI appointed auditor. This arrangement is permitted by section 53 of the Local Government in Scotland Act 2003 (the 2003 Act). All of these parties ('auditors') may thereby be involved in requesting information required for the NFI and the review of audited bodies' arrangements for investigating matches and acting upon instances of fraud and identified weaknesses in internal controls.

1.4.2 Auditors of NHS bodies will be aware of the Partnership Agreement between Boards and NHSScotland Counter Fraud Services (CFS) which requires suspected frauds to be notified to CFS through Boards' Fraud Liaison Officers.

1.5 Background to the National Fraud Initiative

1.5.1 It is vital that public bodies have adequate controls in place to prevent and detect fraud and error. The prevention and detection of fraud by public bodies is a major concern of those bodies as well as Audit Scotland and auditors. Data matching exercises assist appointed auditors in their assessment of the arrangements that have been put in place by audited bodies and assist audited bodies to identify fraud and error.

1.5.2 In 1996, the Audit Commission launched a national fraud initiative to study the extent to which the benefits from a successful data matching exercise, based on local authorities in London, were applicable nationally. The Audit Commission decided in 1998 that the NFI should

form a regular part of the statutory audit in England, conducted at such intervals as the appointed auditor considered necessary.

1.5.3 Audit Scotland undertook successful pilot data matching exercises in Scotland, with the assistance of the Audit Commission's NFI appointed auditor, in 2000/01 and 2002/03. In 2004/05 the exercise was extended to include information from all councils, police and fire boards and selected other public bodies. These data matching exercises in Scotland have now helped to identify around £23 million of fraud, error, overpayments and forward savings.

1.5.4 Data matching involves comparing the extent to which computer records held by one body match against other records held by the same or another body. Computerised data matching techniques are used by the auditor to narrow down the search for duplicate or fraudulent claims made upon audited bodies. A supplying body receives a report identifying instances of matching data within that body's own records and between that body's records and those of other relevant bodies. It is for the supplying body itself to investigate the matches, to detect instances of fraud, over or underpayments and other errors, and to update its records accordingly.

1.6 Purpose of the Code

1.6.1 Audit Scotland is concerned:

- to ensure that its officers, auditors and all bodies involved in data matching conduct or participate in the NFI in a manner which complies with the provisions of the Data Protection Act 1998 ('the DPA') and the general law
- to ensure that all those involved in the NFI follow good practice.

1.6.2 To assist in these objectives, Audit Scotland has drawn up this Code of data matching practice.

1.7 Status and force of the Code

1.7.1 All bodies required by an auditor to supply personal data for the purpose of the NFI should comply with the provisions of this Code. This is to ensure that the NFI is conducted in a manner which meets with the requirements of the DPA and the general law and achieves good practice. It should be noted that the DPA provides for certain exemptions from some of its provisions, and the extent to which these exemptions will apply are set out in the Code.

1.7.2 Where an appointed auditor becomes aware that a body has not complied with the requirements of the Code, he/she will notify the body concerned and seek to ensure that it puts in place adequate measures to meet the Code's requirements.

1.7.3 Bodies which participate or propose to participate in the NFI may reproduce the text of this Code as necessary to facilitate the participation of their organisation in the exercise and to ensure all personnel involved are aware of their obligations under the Code.

1.8 Structure of the Code

1.8.1 The Code comprises of:

- an explanation of the status of the Code and definitions of key terms used in the Code
- principles governing data matching exercises
- practical steps to be adopted by Audit Scotland, auditors and supplying bodies to comply with those principles
- an explanation of how compliance with the Code will be monitored, within Audit Scotland and in relation to supplying bodies
- specific requirements, including good practice letters to data subjects and example declarations for supplying body documentation
- relevant provisions from the Code of audit practice and statute law at Appendices 2-4.

1.9 Adoption and review of the Code

1.9.1 The Code will take effect from the 2006/07 NFI in Scotland exercise, following the conclusion of a formal consultation process. The Code will govern all future data matching exercises in Scotland, until such time as it is reissued.

1.9.2 Audit Scotland intends to review and update the Code periodically in the light of any changes in the law and to reflect users' comments and experience drawn from each data matching exercise.

1.9.3 In addition, the Information Commissioner is welcome to review Audit Scotland's processes during all data matching exercises, and may be invited by supplying bodies to review their procedures. The purpose of this review would be to monitor compliance with data protection principles.

1.10 Queries about the Code

1.10.1 Any questions about this Code, about NFI in Scotland generally or about a particular data matching exercise should be addressed to Russell Frith, Director of Audit Strategy, Audit Scotland, 110 George Street, Edinburgh EH2 4LH. Telephone 0131 477 1234 or email rfrith@audit-scotland.gov.uk.

Part 2. The code of data matching practice

2.1 Status and scope

2.1.1 All bodies supplying data for data matching should observe the provisions of this Code. A copy of the Code has been issued to each supplying body and to auditors. It is also published on Audit Scotland's website.

2.1.2 The Code will be observed by Audit Scotland and auditors when undertaking data matching exercises.

2.1.3 The provisions of the Code set good practice standards that will help organisations to comply with data protection principles.

2.1.4 This Code is not intended to apply to any steps taken by a supplying body to follow up or investigate matches arising from the NFI.

2.1.5 This Code applies for the purpose of the statutory audit of audited bodies in Scotland.

2.2 Definitions

2.2.1 For the purposes of this Code the following definitions apply:

'Appointed auditor' is an auditor appointed by the Commission under section 97 of the 1973 Act or the AGS under section 21 of the 2000 Act to an audited body.

'Auditor(s)' means an appointed auditor, the Audit Commission's NFI appointed auditor or another person approved by the Accounts Commission as part of an arrangement under section 53 of the 2003 Act.

'Audited body' is a public body to which the Commission or the AGS appoints an external auditor.

'Data matching' means the electronic comparison of two or more sets of personal data which have been collected for separate purposes in order to identify any information which is inconsistent for further investigation.

'Non-audited body' is a body other than an audited body but which supplies data to an auditor. Auditors have power to call for data from non-audited bodies under section 100 of the 1973 Act where they relate to a body subject to audit.

'Output' is the computer data file of reported matches in whatever format resulting from processing the data.

'Senior Responsible Officer' is the Chief Executive, Director of Finance or other senior named officer of the supplying body responsible for ensuring compliance with this Code.

'Supplying body' is either an audited or non-audited body which supplies data to an auditor for the purposes of a data matching exercise.

The terms 'data', 'personal data', 'data subject', 'data controller' and 'processing' all have the same meaning as in the Data Protection Act 1998 (DPA').

2.3 Principles governing data matching exercises

2.3.1 To assist in complying with the DPA and the general law the following principles will be observed when undertaking data matching (further details of the practices required of Audit Scotland, auditors and supplying bodies to comply with these principles are detailed in section 2.4):

(a) Participation in data matching exercises carried out as part of the statutory audit is mandatory for:

- all audited bodies governed by the 1973 Act, except where an exemption is given; and
- all other bodies for whom an auditor determines that their data relates to an audited body governed by the 1973 Act, and is required for NFI purposes.

(b) Data will be required by the auditor from all bodies set out in (a) above under section 100 of the 1973 Act.

(c) New areas of data matching will be undertaken on a pilot basis to test the effectiveness of applying data matching to certain data sets. Only where pilots (whether undertaken by Audit Scotland or the Audit Commission) achieve matches that demonstrate a significant level of potential fraud will they be extended nationally in NFI. The terms of this Code will apply in full to pilot exercises taking place within NFI.

(d) Personal data shall only be obtained and processed in accordance with the DPA.

(e) Supplying bodies must inform data subjects that their data may be disclosed for the purposes of auditing in order to identify possible cases of fraud.

(f) Wherever practicable the information required in (e) shall be provided prior to the initial collection of data from data subjects. It should in any event be provided prior to disclosure of the data to the auditor unless it is impractical to do so.

(g) The disclosure of personal data by supplying bodies to the auditor as part of the data matching exercises is for the purpose of identifying possible cases of fraud and consequential correction of any under or overpayments detected.

(h) To ensure fair processing of data, the software, techniques and algorithms used in the data matching exercises are those which are indicative of potential fraud and/or under or overpayments only, and will be refined in the light of practical experience.

(i) No assumption should be made that matches are fraudulent. Auditors and audited bodies should review output to eliminate coincidental matches, and concentrate on potentially fraudulent cases. In order to do so they will need to identify and correct those cases where errors have occurred.

(j) The data provided by supplying bodies should be the minimum required to undertake the matching exercise and report the results. This will be set out in a handbook. The relevant handbook will prescribe the data that is sufficiently adequate and relevant (but not excessive) to enable individuals to be accurately identified during the data matching process and from the data matching output, so as to give confidence in the data matching process.

(k) Data provided by supplying bodies must be of a good quality in terms of accuracy and completeness. Prior to supplying data for matching, bodies must ensure that the personal data are as accurate and up to date as possible.

(l) Data should be destroyed promptly once no longer required, unless needed by supplying bodies as working papers for the purposes of audit, or for the purpose of continuing investigations or prosecution.

(m) Data should not be disclosed in the course of data matching exercises to parties beyond the defined scope of the NFI, unless there is specific legal authority for so doing.

(n) Security arrangements for handling and storage of data by all involved in the NFI should ensure that:

- specific responsibility has been allocated to one or more managers for security of data
- security measures take appropriate account of the physical environment in which data is held, including the security of premises and storage facilities
- there are logical controls to restrict access appropriately to electronic data
- all staff with access to data are given appropriate training.

2.4 Practical steps required to comply with the data matching principles

2.4.1 The practices which should be adopted by Audit Scotland, auditors and supplying bodies to comply with these principles are summarised in sections 2.5 – 2.11, regarding:

- governance arrangements
- requirements for fair collection and disclosure of personal data

- data handling
- intermediate processing
- output control
- access control
- data back-up.

2.5 Governance arrangements

2.5.1 The Chief Executive, the Director of Finance or equivalent senior named officer of each supplying body will act as Senior Responsible Officer for NFI purposes. The Senior Responsible Officer will authorise named officers responsible for data handling, for following up investigations and to act as key contacts with the auditor, and will ensure they are suitably qualified and trained for their role.

2.5.2 For each data matching exercise, a handbook will be distributed to all supplying bodies, setting out the detailed requirements for participation in NFI. The most up-to-date handbook can be found on Audit Scotland's website at http://www.audit-scotland.gov.uk/nfi/nfi.htm

2.5.3 The handbook will contain:

- a list of the responsibilities of the nominated officers at the supplying body
- a supplying body statistics return (requesting key facts and figures for each system to be matched)
- data specifications for each system (listing the minimum data to be provided by the supplying body to enable data matching and output of sufficient quality)
- preferred data formats and media
- a data checklist to be submitted with each dataset
- a timetable for processing
- a data protection compliance return
- an explanation of the significance of matches between particular data sets and the approach which should be taken in carrying out investigations.

2.5.4 Supplying bodies must have procedures in place for dealing appropriately with requests from data subjects for access to their data, and for complaints about the inclusion of their data in a data matching exercise. If requests for access to data are received during the matching exercise, requests that the auditor is best placed to deal with should be passed on promptly so the auditor can respond appropriately.

2.5.5 The Information Commissioner maintains a public register of data controllers. Each register entry includes the name and address of the data controller, and the purposes for which data is processed (identifying the data subjects and recipients for each purpose). It is the responsibility of all supplying bodies to ensure their notification to the Information Commissioner includes auditors as recipients against the appropriate purpose(s).

2.5.6 A Notification handbook is available from the Information Commissioner, which sets out how to complete the required Notification form. Notification templates are available from the Information Commissioner for local authorities, NHS and other public bodies. These include the disclosure of personal data to auditors in certain circumstances. If these templates are not used by a supplying body, the body must still ensure its register entry covers disclosures to auditors.

2.5.7 All auditors must be registered as data controllers for the purpose of NFI.

2.6 Requirements for fair collection and disclosure of personal data

2.6.1 Collection of new data. For data processing to be fair, the first data protection principle under the DPA requires data controllers to inform data subjects of the identity of the data controller, the purpose or purposes for which the data may be processed, and any further information which is necessary. Subject to certain exemptions, which are described later, where practicable this should be done at the time of the original collection of the data from data subjects. Supplying bodies collecting new personal data that they know will be used for the purposes of NFI must inform data subjects at the point of data collection that their personal data may be disclosed for the purposes of auditing in order to identify possible cases of fraud.

2.6.2 Appendix 1 contains a standard fair collection notice for inclusion on benefit and other application forms. The notice covers the use of personal data in anti-fraud and data matching initiatives conducted both by the body collecting the data and by the auditor. Data which have been collected on the basis of the recommended fair collection notice (or equivalent) may be disclosed to the auditor for the purposes of the NFI.

2.6.3 Use and disclosure of existing data. Some of the data to be disclosed for the purposes of data matching may already have been collected without a fair collection notice having been provided at the

time of the original data collection. In the case of the NFI, exemptions are available under the DPA from the requirement to provide fair collection notices at the time of the original data collection.

2.6.4 The principal exemptions on which NFI relies are in sections 29 and 35 DPA. For those bodies in respect of which participation in data matching is mandatory, the exemption under section 35 DPA applies. The data from these bodies are required to be provided to the auditor relying on powers in section 100 of the 1973 Act (see principle (a) under 2.3.1 above). Section 35 exempts personal data from the non-disclosure provisions of the DPA where they are required under any enactment.

2.6.5 The exclusion of existing data from the exercise where fair collection notices were not provided at the time of the original collection is likely to prejudice the prevention or detection of crime, and to this extent the exemption in section 29 applies.

2.6.6 Retrospective fair collection notices. In the limited number of cases where it is not practicable to furnish data subjects with a fair collection notice at the time of the original collection of the data, retrospective fair collection notices should be given at the earliest reasonable opportunity to every individual data subject concerned (and in any event before disclosure to an auditor) unless it is impracticable to do so. One example of when it might be impractical is where the current address is not known. Giving notice will enable all data subjects to know that their data is being included in data matching and to take appropriate steps if they consider the use is unjustified or unlawful in their particular case.

2.6.7 Considerations in different cases. In the case of applications made by data subjects to the body concerned, a fair collection notice can be included in the application form intended for use by the data subject (see 2.6.2). Such notices will have the effect of deterring fraud as well as informing about the inclusion of the data in data matching.

2.6.8 In other cases (occupational pensioners, employees, tenants etc), supplying bodies already communicate formally at least once a year in the form of a newsletter or payslip etc. Fair collection notices should be included in these communications, which should be sent to named individuals in advance of each NFI exercise, to ensure that all data subjects are advised. This will avoid the cost of a separate mailing. A number of supplying bodies have already adopted this approach and a copy of a good practice example appears in this Code at Appendix 1.

2.6.9 In all cases communication with data subjects must be clear, prominent and, subject for example to paragraph 2.3.1(f), timely.

2.6.10 The submission of data to the auditor must be accompanied by a declaration from each body confirming compliance with the fair collection requirements set out in this Code. The appointed auditor will check that the requirements have been adhered to and, where necessary, will agree the steps necessary for the body to meet any concerns.

2.6.11 Deceased persons. Some of the data used for data matching purposes in NFI relates to deceased persons. Although not classed as personal data under the DPA, common law rules of confidentiality may restrict disclosure in certain circumstances. Particular care and sensitivity should be taken in dealing with data concerning deceased persons throughout the exercise, but particularly in the case of investigation of matches, to avoid any unnecessary distress and embarrassment.

2.7 Data provided by supplying bodies

2.7.1 The data provided by supplying bodies must be of good quality in terms of its accuracy and completion. Processing of inaccurate data could mean that the supplying body is in breach of data protection and/or defamation law. Before submission of data to the auditor, errors identified from previous data matching exercises should be rectified, and action taken to address recommendations in data quality reports provided to the supplying body. The supplying body's key contact should check the readability of the data before despatch. This will help minimise the time that an auditor retains the data.

2.7.2 Data provided by the supplying bodies should be despatched to the auditor by courier or special delivery. In Scotland the matching is undertaken on behalf of auditors by the Audit Commission's NFI appointed auditor and supplying bodies send their data directly to the Audit Commission's contractor.

2.7.3 All data in whatever form will be logged on receipt and stored securely in a fire-proof safe. All data stored electronically will be held on a secure, password-protected computer system maintained in a secure environment.

2.7.4 Data submitted as part of the NFI will not be passed to any third party (ie a person other than the bodies participating in NFI and the firm contracted to provide data matching services) by auditors or their agents, unless required by law.

2.7.5 All original data submitted to the auditor in whatever form (tape cartridges, cassettes, diskettes, hardcopy and CD-ROMs) will be destroyed and rendered irrecoverable by the auditor after all processing and re-runs are completed and all queries resolved. This will be done promptly and, in any event, within six months of the conclusion of the exercise.

2.8 Intermediate processing

2.8.1 The firm processing data for the Audit Commission will do so under a contract in writing which imposes requirements as to technical and organisational security standards so as to meet ISO 17799, and under which the firm may only act on instructions from the Audit Commission.

2.8.2 All intermediate data used in data matching exercises will be erased and rendered irrecoverable in the same timetable as original data (see paragraph 2.7.5).

2.9 Output control

2.9.1 All output from data matching exercises (if on CD-ROM) should be distributed by courier or sent by special delivery to the Senior Responsible Officer (ie the Chief Executive, Director of Finance or equivalent named senior officer of the supplying body), together with a pack comprising: investigation guidelines, good practice protocols, output overview, feedback forms and a list of key contacts. From 2006/07, distribution is planned to be web-based, which should eliminate distribution logistical issues and strengthen access controls to data.

2.9.2 All output from data matching exercises will be password protected and should be stored securely in a locked facility in a secure environment or on a secure, password-protected computer system as the case may be.

2.9.3 The circumstances surrounding an individual match will be considered by an investigator at the supplying body before any decision is made consequent on that match. Investigating officers should refer to the investigation guidelines included in the CD-ROM (or web-based application).

2.9.4 Supplying bodies may retain any CD-ROM disclosed to them which contains data matches as working papers if required for the purposes of audit, or for the purpose of continuing investigations or prosecution. Supplying bodies should discuss with their appointed auditor what should be retained in their individual case, and subject to that, should ensure that data no longer required is destroyed promptly.

2.9.5 Auditors will review output so that the data matching techniques and algorithms used can be refined for future exercises. Similarly, the data requirement specifications should be reviewed and refined.

2.9.6 No copies of any output should be retained longer than necessary by an auditor, except a single set of the 'match keys' in magnetic form, held securely offline by the Audit Commission. This is solely for the purpose of preventing duplication of matches in any subsequent data matching exercises.

2.10 Access control

2.10.1 All persons handling data as part of the data matching process should be made aware of their data protection and security obligations under the DPA and this Code and should be given appropriate training as necessary. Such staff should be subject to strict access authorisation procedures. Breach of authorisation procedures should attract appropriate disciplinary sanctions.

2.10.2 Access to data held in any form should only be granted to named individuals (auditors, approved staff within the firm that undertakes the processing, or named officers of the supplying bodies). The Senior Responsible Officer should ensure that each type of output is disclosed only to appropriate officers by use of the installation menu provided for that purpose.

2.10.3 All computers used to process the data should have appropriate physical and logical access controls so as to limit access only to the named individuals. These controls should be subject to review by the appointed auditor.

2.10.4 File permission for all data files should be set so as to limit access at any level to the appropriate named individuals. Where a breach of security occurs, or is suspected, authorised users should be given new passwords or required to change their passwords as soon as possible.

2.11 Data back-up

2.11.1 All data submitted as part of NFI should be backed up by the Audit Commission at appropriate intervals, but not more often than is reasonably necessary. Back-ups will be subject to the same security, destruction and access controls as the original data.

Part 3. Monitoring compliance with the Code of data matching practice

3.1. Section 51(7) of the DPA provides that the Information Commissioner may, with the consent of the data controller, assess any processing of personal data for the following of good practice. Audit Scotland would welcome any review of NFI in Scotland compliance with the Act. To enable the Information Commissioner to do this it would also be necessary to assess compliance of those bodies supplying personal data. For this reason all bodies supplying data for the purposes of NFI should accede to any reasonable request by the Information Commissioner to carry out an assessment of their processing of personal data. Such an assessment would be expected to be designed only to monitor compliance with the data protection principles.

Appendix 1. Specimen fair processing notices

Good practice example of notice to be included in application forms
(see paragraphs 2.6.1 and 2.6.7 of the Code)

'This authority is under a duty to protect the public funds it administers, and to this end may use the information you have provided on this form for the prevention and detection of fraud. It may also share this information with other bodies responsible for auditing or administering public funds for these purposes.'

Good practice example letter to data subjects
(see paragraph 2.6.8 of the Code)

This example has been drafted for pensioners; the words in [square brackets] should be amended accordingly for employees, tenants etc.

Dear (name [of pensioner])

I am writing to let you know that (name of audited body) is participating in an exercise to ensure that public money is being spent properly.

The (name of audited body) is under a duty to protect the public funds it administers. It may share information provided to it, with other bodies responsible for auditing or administering public funds, in order to prevent and detect fraud.

Our auditors are appointed through Audit Scotland and they currently require us to participate in an anti-fraud initiative. For this initiative, we are providing details of [pensioners] to the auditors so that they can compare these with information provided by other public bodies. This will ensure that [no pensions are being paid to persons who are deceased or are no longer entitled to them, and that occupational pension income is being declared when housing benefit is applied for].

Sometimes wrong payments are made because of genuine error. Previous exercises have uncovered instances of [pensioners] receiving too little [pension], resulting in the payments to [pensioners] being increased. These exercises, therefore, help ensure the best use of public funds.

You do not need to respond to this letter. You may be contacted again in the future if the exercise suggests you are not receiving the correct amount of [pension]. However, if you do have any questions, you should contact (name of NFI key contact).

Appendix 2. The Code of audit practice

1. Audit Scotland prepares a Code of audit practice prescribing the way in which appointed auditors are to carry out their functions under the 1973 and 2000 Acts. The Code of audit practice is approved by the Accounts Commission and the Auditor General. The current Code was approved and published in 2001. It defines the scope of auditors' responsibilities, of which some of the most relevant are set out in this appendix. Although this version of the Code is due to be revised, the respective responsibilities of auditors and audited bodies are, in any event, consistent with applicable law and relevant auditing standards.

2. Data matching is an efficient audit technique which assists auditors in fulfilling their responsibilities, particularly in relation to the following provisions of the Code of audit practice:

- The Code requires auditors to give an opinion on the audited body's financial statements and, among other things, 'review and.... report findings on corporate governance arrangements as they relate to... the ...audited body's review of its systems of internal control... [and]... the prevention and detection of fraud and irregularity' and whether the audited body has made proper arrangements for securing economy, efficiency and effectiveness in its use of resources. Data matching results provide evidence to auditors of both frauds and under and overpayments, helping them to form a judgment as to whether the audited body has adequate arrangements in place.

- The Code also requires auditors to 'provide reasonable assurance that..... the financial statements are free from material misstatement, whether caused by fraud or other irregularity or error.' A significant number of over or underpayments identified using a data matching technique may give the auditor reason to believe that there has been a material misstatement of the accounts. This may in turn lead to audit recommendations to improve the systems of internal control in operation in the audited body.

Extracts from the Code of audit practice

Introduction

Background

4. The special accountabilities attached to the conduct of public business and use of public money mean that audit in the public sector requires to be planned and undertaken from the wider perspective of providing not only assurance on the financial statements (and statements of internal control, where appropriate) prepared by public bodies, but also providing a view on matters such as regularity (or legality), propriety and use of resources in accordance with the concepts of "value for money" and best value. In so doing, it contributes positively to the corporate governance arrangements of public bodies that enable them to operate effectively with due regard to regularity, propriety, good value for money and improved performance.

5. Accordingly, whilst the basic principles of a financial statements audit are common to both the public and private sectors, external auditors in the public sector in addition to giving an independent and objective opinion on public bodies' financial statements also review, and report on, aspects of the arrangements made by the body to ensure the proper conduct of its affairs and to manage performance and use of resources.

General principles

Confidentiality

29. The auditor should comply with relevant professional and ethical guidance and take all reasonable steps to ensure that they and their staff treat as confidential all information received or obtained during the course of the audit. The auditor should recognise that in the public sector there is a greater degree of transparency expected and take particular care in the presentation of information in documents that may be expected to enter the public domain. Auditors should also have regard to the terms of any Memoranda of Understanding or similar documents entered into by the Accounts Commission or Auditor General with inspectorates or similar bodies.

Audit framework

Approach

30. The auditor should carry out the audit in a professional manner, as efficiently and effectively, and in as timely a way as possible. Therefore, in exercising professional judgement in framing an audit approach to meet the requirements of this Code, the auditor should:

(a) plan and perform the audit, determining where to direct work and allocate resources, having regard to the concepts of materiality and significance, to ensure that the audit is tailored to the circumstances of the audited body

(b) recognise that each part of the audit needs to be viewed in the context of the whole, ie, that no single part stands alone and work in relation to one element informs work in relation to others

(c) seek to establish effective coordination arrangements with the audited body's internal auditors and, if relevant, auditors of other public

sector bodies, inspectors or review agencies, and Audit Scotland

(d) adopt a constructive and positive approach to audit work, supporting and where appropriate encouraging change in the audited body's practices, while providing independent scrutiny and assurance, and fulfilling statutory and professional obligations

(e) report in such a way as to inform the audited body's members and management of matters of significance arising from audit work and of the nature and grounds for concerns, indicating corrective action that may be required

(f) establish arrangements to review whether or not the audited body has properly considered any matters identified during the audit or those of previous periods and, where appropriate, has implemented agreed actions.

Reporting the audit

40. Reports from the auditor are the primary means by which the results of audit activity are brought to the attention of senior management of the audited body, elected or board members and other stakeholders, including the Scottish Parliament and the public.

41. The mechanisms for reporting the results of the audit will vary according to the statutory and financial frameworks applicable to the audited body. However, it is expected that the auditor will as a minimum provide:

- a report or certificate to the audited body and, as appropriate, the Auditor General and Scottish Parliament or Accounts Commission that the audit of the financial statements has been completed in accordance with applicable statutory requirements and including an opinion on those financial statements;
- reports or letters addressed to management of the audited body and, if appropriate, members and copied to, as appropriate, the Auditor General or Controller of Audit, bringing to their attention matters arising from the auditor's work under this Code;
- an annual audit report addressed to the audited body and, as appropriate, the Auditor General or Controller of Audit.

Annual audit report

47. The purpose of the annual audit report is to set out the scope, nature and extent of the audit work that has been carried out for the period and to summarise the auditor's opinions or conclusions and, where appropriate, significant issues arising from the work. In broad terms, the report should be used to:

- expand upon any qualification in the auditor's report or certificate in relation to the financial statements, explanatory paragraph or reference to the audited body's failure to comply with a statutory requirement
- report or direct attention to any matters of significance arising from the audit process
- set out, as appropriate, the respective responsibilities of management and the auditor in relation to issues associated with regularity, propriety and performance management
- note the action taken or the auditor's recommendation as to action required to be taken by members or management to resolve any issues or areas of concern arising in the period under review and previous periods.

Financial statements

The auditor's role

59. The auditor is required to audit the financial statements and to give an opinion:

- whether (as appropriate depending on the financial reporting framework) they give a true and fair view or present fairly the financial position of the audited body and its expenditure and income (or equivalent) for the period in question
- whether they have been prepared properly in accordance with relevant legislation, applicable accounting standards and other reporting requirements
- except for local government bodies, on the regularity of the expenditure and receipts.

60. In carrying out this responsibility, the auditor provides reasonable assurance that, subject to the concept of materiality, the financial statements:

- are free from material misstatement, whether caused by fraud or other irregularity or error
- comply with the statutory and other requirements applicable to them
- comply with relevant requirements for accounting presentation and disclosure.

61. In forming the opinion and in addition to the requirements of accounting standards, it is expected that the auditor will have considered compliance with such requirements on the form of financial reporting as may be applicable.

62. In carrying out an audit of financial statements the auditor is required to comply with Statements of Auditing Standards and to have regard to any relevant Practice Notes and other guidance and advice issued by the Auditing Practices Board.

Corporate governance arrangements

Prevention and detection of fraud and irregularities

80. It is the responsibility of the audited body to establish arrangements to prevent and detect fraud and other irregularity. As part of its corporate governance framework and control systems, it needs therefore to put in place proper arrangements for:

- developing, promoting and monitoring compliance with standing orders and financial instructions;
- developing and implementing strategies to prevent and detect fraud and other irregularity;
- receiving and investigating allegations of breaches of proper standards of financial conduct or fraud and irregularity.

81. The auditor's responsibility in this area is discharged by reviewing and, where appropriate, examining evidence that is relevant to these arrangements, particularly in relation to aspects of internal financial control such as segregation of duties, authorisation and approval processes and reconciliation procedures.

82. While it is not the auditor's responsibility to prevent or detect fraud or irregularity, the auditor should at all times be alert to the potential for breaches of procedures, and of fraud and other irregularity. If weaknesses in aspects of the audited body's arrangements which might facilitate such instances, are identified or notified in the course of audit work, the auditor should report them timeously to management of the audited body and those charged with governance responsibilities. Indications of fraud and other irregularity, from whatever source and whatever the potential value involved, should be followed up promptly. In most cases, the auditor will discharge this responsibility by informing the appropriate level of management at the audited body and recommending that they take an appropriate course of action, which, according to circumstances, might include referral to another agency.

83. The audit of the financial statements should be planned so that there is a reasonable expectation of detecting misstatements arising from fraud or other irregularity that are material in relation to those financial statements. This is considered further in relation to the audit of the financial statements (paragraphs 58 to 68).

84. Fraudulent transactions cannot, by definition, be regular since they are without proper authority. In the circumstances of proven or suspected fraud, the auditor requires to consider the impact on the regularity part of the opinion on the financial statements.

85. Auditors are required to make submissions of instances of fraud and irregularity to Audit Scotland in accordance with its requirements and to review related reports circulated by Audit Scotland, drawing conclusions therefrom and taking action as appropriate.

Performance audit

Use of resources

103. As part of their statutory responsibilities, the Auditor General and the Accounts Commission will procure through Audit Scotland examinations of the use of resources and publish reports or guidance. These performance audit reviews, which may be undertaken at a specific body, within a sector (such as the NHS) or on a Scotland-wide basis, promote good management practice and the best use of public money in service delivery. Depending upon the sector involved and the nature of the review this work may be carried out by the auditor, central Audit Scotland staff or by others.

Appendix 3. Local Government (Scotland) Act 1973

Section 100 – Auditors' right to documents and information

(1) An auditor shall have right of access at all reasonable times to all such documents relating to the accounts of a local authority as it appears to him to be necessary to examine for the purpose of auditing those accounts under this Part of this Act and shall be entitled to require from any officer of that authority or any other person holding or accountable for any such document such information and explanation as he things necessary for the said purpose and, if he thinks it necessary for providing any such information or explanation, to require any such officer or other person to attend before him in person and produce any such documents.

(1B) Without prejudice to subsection (1) above, the auditor shall be entitled to require any officer, former officer, member or former member of an authority whose accounts are required to be audited in accordance with this Part of this Act and any person who, by arrangement or agreement with the authority or body, is discharging any function of the authority or body to give him such information or explanation as he thinks necessary for the purposes of the audit and, if he thinks it necessary, to require any of the persons mentioned above to attend before him in person to give the information or explanation or, where that person is a body corporate, to require that person to appoint a representative to attend before the auditor for that purpose.

(2) Without prejudice to subsections (1) and (1B) above, every local authority shall provide an auditor with every facility and all information which he may reasonably require for the purpose of auditing their accounts and every person who, by arrangement or agreement with a local authority, is discharging any function of the authority shall make that provision for the purpose of the auditing of the authority's accounts.

(3) If any person wilfully or negligently fails to comply with any requirement of an auditor under subsection (1) above, he shall be guilty of an offence and shall be liable on summary conviction to a fine not exceeding £100 and to an additional fine not exceeding £20 for each day on which the offence continues after conviction thereof.

NB: The reference to 'any other person' in section 100(1) permits information to be obtained, for example, from the Student Awards Agency for Scotland and other public bodies. NFI in Scotland 2004/05 identified more than 200 students who were inappropriately claiming housing benefit from councils.

Appendix 4. Local Government in Scotland Act 2003

Section 53 – Qualification of and assistance for Accounts Commission auditors

(3) Auditors appointed under section 97 of the 1973 Act by the Accounts Commission (whether or not officers of the Commission) may be assisted by having such of their functions as may be specified in arrangements approved by the Commission carried out by other persons so specified or so referred to.

(4) Such arrangements may apply generally or to a particular case or cases.

NB: The Accounts Commission has approved arrangements for appointed auditors to be assisted, for the purpose of the NFI, by the Audit Commission's NFI appointed auditor and officers from Audit Scotland.

Appendix 5. Relevant parts of sections 29, 35 and 55 of the Data Protection Act 1998

Section 29 Crime and taxation

(1) Personal data processed for any of the following purposes:

(a) the prevention or detection of crime,

(b) the apprehension or prosecution of offenders, or

(c) the assessment or collection of any tax or duty or of any imposition of a similar nature,

are exempt from the first data protection principle (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3) and section 7 in any case to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.

(3) Personal data are exempt from the non-disclosure provisions in any case in which:

(a) the disclosure is for any of the purposes mentioned in subsection (1), and

(b) the application of those provisions in relation to the disclosure would be likely to prejudice any of the matters mentioned in that subsection.

Section 35 Disclosures required by law or made in connection with legal proceedings etc

(1) Personal data are exempt from the non-disclosure provisions where the disclosure is required by or under any enactment, by any rule of law or by the order of a court.

Section 55 Unlawful obtaining etc of personal data

(1) A person must not knowingly or recklessly, without the consent of the data controller,

(a) obtain or disclose personal data or the information contained in personal data, or

(b) procure the disclosure to another person of the information contained in personal data.

(2) Subsection (1) does not apply to a person who shows:

(a) that the obtaining, disclosing or procuring:

(i) was necessary for the purpose of preventing or detecting crime, or

(ii) was required or authorised by or under any enactment, by any rule of law or by the order of a court,

(b) that he acted in the reasonable belief that he had in law the right to obtain or disclose the data or information or, as the case may be, to procure the disclosure of the information to the other person,

(c) that he acted in the reasonable belief that he would have had the consent of the data controller if the data controller had known of the obtaining, disclosing or procuring and the circumstances of it, or

(d) that in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest.

(3) A person who contravenes subsection (1) is guilty of an offence.

(4) A person who sells personal data is guilty of an offence if he has obtained the data in contravention of subsection (1).

(5) A person who offers to sell personal data is guilty of an offence if:

(a) he has obtained the data in contravention of subsection (1), or

(b) he subsequently obtains the data in contravention of that subsection.

(6) For the purposes of subsection (5), an advertisement indicating that personal data are or may be for sale is an offer to sell the data.

(7) Section 1(2) does not apply for the purposes of this section; and for the purposes of subsections (4) to (6), 'personal data' includes information extracted from personal data.

(8) References in this section to personal data do not include references to personal data which by virtue of section 28 (or 33A) are exempt from this section.

Code of data matching practice

National Fraud Initiative in Scotland

If you require this publication in an alternative format and/or language, please contact us to discuss your needs. It is also available on our website: **www.audit-scotland.gov.uk**

Audit Scotland
110 George Street
Edinburgh EH2 4LH

Telephone
0131 477 1234
Fax
0131 477 4567

www.audit-scotland.gov.uk