

Department of Work & Pensions
Information & Analysis Directorate

Preliminary Audit of IAD Systems

11th January 2005

Enterprise Privacy
Group
Old Bank House
59, High Street
Odiham
Hants RG29 1LF
T: +44 (0)1256 702325
F: +44 (0)1256 702375

SUMMARY

This is the final report on the third-party preliminary audit and risk assessment of the Department of Work & Pensions' (DWP) Information & Analysis Directorate (IAD) systems conducted by the Enterprise Privacy Group. The purpose of this report is to detail the findings, conclusions and recommendations arising from the review.

The DWP and IAD documentation appears to be both comprehensive and largely complete - certainly when compared with our experience of Data Protection documentation in other large organisations. We believe a full audit would conclude that the documentation is legally satisfactory and we therefore have no hesitation in confirming its adequacy.

Compliance with documentation is largely excellent. IAD staff generally demonstrate a genuine commitment to carrying out their privacy duties, and are keen to observe Data Protection principles. However, our assessment of IAD's Data Protection system raises concerns over three key areas of procedure and operation, namely:

- Data Protection Strategy: continued effort is needed to implement the stated commitment to good privacy practices;
- Staff Awareness: despite their enthusiasm, many staff lack the knowledge they require to put policies into practice, and will require ongoing training and education to achieve and maintain a high standard of Data Protection practice;
- System Audit and Review: Data Protection audit appears to be a relatively new function within IAD, and there is a need for further work to ensure that it becomes embedded in normal operations.

We are satisfied that these issues will be adequately addressed by the creation of the DSU7 Data Protection team, and IAD's new work on Data Protection awareness and audit that has already commenced.

At some key levels, the data protection system and data protection compliance remains at odds with the high expectations for privacy protection, security and safeguards set by the Department's public statements regarding the Longitudinal Study and data matching. There are also significant risks that persist at the broader level of public relations because of inconsistencies in published statements and in organisational process. Public commitments in areas such as transparency must be rigorously observed.

Nevertheless, the compliance audit score we have given to IAD (based on the final risk assessment) is on the very high end of the scale. Specific concerns notwithstanding, we believe it is likely that IAD compliance would be awarded a 'green light' in any subsequent audit. This conclusion is, we believe, a realistic one, even though audit scrutiny of any large-scale public sector system can be unusually critical. The prospect of passing a full audit will depend largely on the development of internal management and oversight arrangements that are practical and effective, as well as development of staff awareness that is deeply embedded and resilient.

TABLE OF CONTENTS

Part 1.	Introduction	
	Background	3
	About this report	3
	Purpose of this report	3
	Scope of this report	3
	Our approach	4
	Scope of the EPG review	4
	Legal advice	4
	What this report contains	4
Part 2.	Overview of key findings and recommendations	
	Introduction	5
	Context of the review	5
	Progress since the First Stage Report	5
	High level audit indicators - the 'dashboard'	6
	Summary of findings and recommendations	7
Part 3.	Adequacy assessment	
	Introduction	9
	Adequacy assessment of DWP documentation	9
Part 4.	Compliance assessment	
	Introduction	10
	Background	10
	The assessment	10
	Physical aspects	17
	Behaviour patterns	17
	Ethics Committee	17
Appendix A.	Audit schedule	
	Documents reviewed	18

PART 1. INTRODUCTION

Background The Enterprise Privacy Group (EPG) was commissioned by the Department for Work and Pensions' (DWP) Information and Analysis Directorate (IAD) to conduct a pre-audit on IAD systems to measure the levels of compliance with requirements of the Data Protection Act.

This requirement arose from the need to confirm the legality of processing as part of the DWP's Work and Pensions Longitudinal Study, as announced by the Secretary of State for Work and Pensions in December 2003.

About this report This is our final report on the third-party preliminary audit and risk assessment of IAD systems. The findings and recommendations are based on interviews, site visits and documentation reviews up to and including the publication date. The report incorporates the findings and recommendations of our **First Stage Report** of 7th July 2004 together with subsequent work.

Purpose of this report The purposes of this document are to:

- detail our findings and conclusions arising from the review;
- set out specific recommendations for further action that are believed to be necessary if IAD is to ensure a continued very high standard of information protection.

The report is intended to supplement the **First Stage Report**, and for the sake of brevity some information in that report has not been duplicated here.

Scope of this Report The scope of this report addresses the following key elements of our work programme:

- adequacy assessment: to check that any documented Policies, Codes of Practice, Guidelines and Procedures meet the requirements of the Data Protection Act 1998. A more detailed assessment is provided in the **First Stage Report**;
- compliance assessment: to ensure that the DWP is in fact operating in accordance with its documented Policies, Codes of Practice, Guidelines and Procedures;
- privacy template development: to ensure that IAD's management team has a clear understanding of the key compliance issues for which they are responsible;
- development of overall report on recommendations and actions.

The following elements of the agreed work programme are omitted from this document, but covered in the **First Stage Report**:

- planning and risk assessment;
- preliminary compliance assessment;
- development of pre-audit guidelines: covered in **Appendix 2** of the **First Stage Report**.

Two elements of the work programme have been dropped from the scope of work:

- options for technical implementation for best practice: this was deferred to a new piece of work that commenced early in 2005. That project will create a 'self-certification' scheme, with the objective of integrating awareness and audit processes using the Directorate's Lotus Notes platform. EPG is managing that project;
- comparative best practice assessment - UK and abroad: this was dropped from the scope of work due to necessary restrictions on time and travels costs.

Our approach

Our process is derived from the stages and benchmarks set out in the Information Commissioner's Audit Manual together with additional procedures as advised by the Commissioner's office. This approach ensures compatibility with any subsequent audit.

To gather the information we interviewed DWP staff over a five-month period and analysed relevant DWP documents, which are listed in **Appendix A**. The DWP documents and policies were assessed against the requirements of the UK Data Protection Act, the European Data Protection Directive (1995), the European Convention on Human Rights. They were also checked against a number of Codes and Opinions published by the Information Commissioner, including the Employment Practices Data Protection Code and Durant vs FSA.

The findings were then check-listed against the 47 criteria set out in the Information Commissioner's Data Protection Audit Manual. These are provided in **Appendix 2** of the **First Stage Report**.

Scope of the EPG review

The EPG review was confined to operations within IAD, and to documentation that relates to those operations. The review did not cover other parts of DWP, nor did it include services provided by third party organisations.

The scope of the review did not include confirming the validity of information provided. Where documents were provided to us, such data was accepted at face value and was not cross-checked or challenged.

Legal advice

Please note that this report has not been scrutinised by legal experts. Any use of the recommendations in this report should be supported by independent legal advice where appropriate.

What this report contains

This report contains the following sections:

Part 2. Overview of key findings and recommendations

A summary of the key findings and recommendations arising from the review, including the high-level audit results.

Part 3. Adequacy assessment

An assessment of the suitability and availability of relevant documentation.

Part 4. Compliance assessment

An assessment of IAD compliance with the Data Protection Act.

Appendix A. Audit schedule

A list of the documents provided to EPG as part of the review.

PART 2. OVERVIEW OF KEY FINDINGS AND RECOMMENDATIONS

Introduction This section describes progress since our **First Stage Report**, summarises the key findings and recommendations arising from our review, and provides a 'dashboard' high-level audit view of IAD compliance with Data Protection issues.

Context of the review We are very much aware that within the public sector in the UK there is little precedent for the work being undertaken by IAD. The responsiveness of IAD to issues raised by this preliminary audit indicates that the Directorate views human relations and Data Protection as integrated issues. This is an important and refreshing perspective that we believe will accelerate implementation of standards of excellence in Data Protection.

Progress since the First Stage Report The **First Stage Report** of 7th July 2004 was largely positive in its findings, and included a number of recommendations to ensure that IAD obtains an overall finding of adequacy in its handling of personal information. The IAD management team was quick to respond to these recommendations. In consequence, Data Protection standards and processes within IAD have evolved substantially since we commenced the EPG review. The outcome can be measured both through the development of documentation and by the development of organisational processes.

These initiatives, in our view, are fuelled by a demonstrable commitment by senior management to the protection of personal information. The extent of this commitment is unusual. Motivation at this level is an essential element in the drive to create a culture shift within the organisation. Having acknowledged this challenge, substantial work must still be undertaken within IAD to achieve that culture shift. A systematic approach must be taken to capture hearts and minds.

We have also observed a perceptible shift in attitude and practice throughout IAD. This pleasing outcome indicates that ongoing efforts to change 'hearts and minds' are making inroads into departmental culture. As we observe later in this report, this outcome must be supported by endemic changes to IAD's approach to staff awareness development and internal audit.

We had expressed concern in the **First Stage Report** that levels of physical environment in the Newcastle site might be inadequate to maintain the levels of security stipulated in the documentation. We are pleased to learn that these shortcomings are being addressed, to the extent that plans have been made to relocate teams to more secure premises where required.

High level audit indicators - the 'dashboard'

In our **First Stage Report**, we scored the data protection compliance of a variety of key sections, functions and outputs of the IAD. The results were presented as a 'dashboard' using a traffic light code, as follows:

- **Green:** Adequately compliant or moving to Best Practice;
- **Amber:** Probably compliant, but requiring attention;
- **Red:** Either a significant risk of non-compliance or not enough information currently available to make a judgement.

This process has been repeated to reflect current levels of compliance, which are shown in **Figure 1** below. Those areas where we believe there has been an evident improvement in adequacy or compliance since the **First Stage Report** are indicated with dashed lines: - - - - -

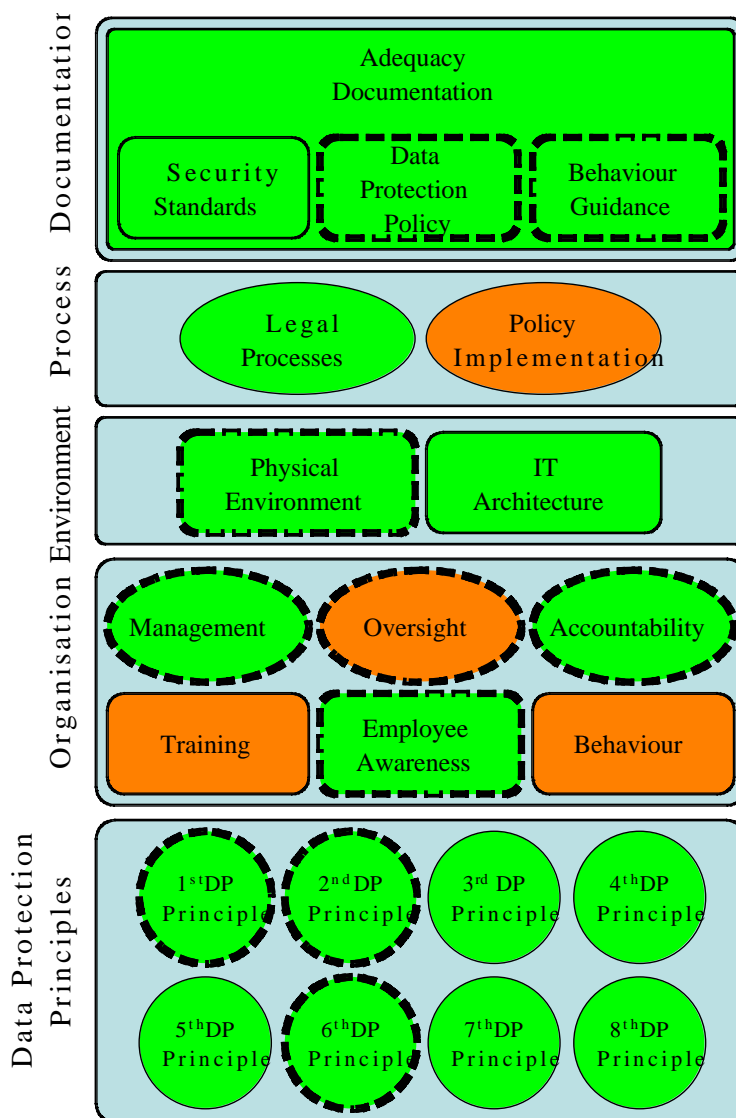


Figure 1: DWP-IAD High level audit indicators - the 'dashboard'

Of the ten areas that have demonstrated an improvement, the most notable are Management, Accountability, Awareness and the First Data Protection Principle, all of which have switched from 'Red' to 'Green' ratings.

Summary of findings and recommendations

Our key findings and recommendations are summarised in **Table 1** below. These findings and recommendations supersede those of the **First Stage Report**, and they reflect the numerous positive changes initiated by IAD management since the start of our work.

Whilst several of these observations carry associated recommendations, we should point out that such deficiencies do not lead to an overall negative finding. There is every reason to believe that a comprehensive audit - even under present circumstances - will find favourably at all levels of operation and procedure. However, in view of the very high standards set by IAD management we will award only a provisional 'green' on some aspects of compliance.

Issue	Finding	Recommendation
Data Protection Policy	Whilst the necessary Data Protection policies and standards are in place, the overall strategy for implementing and managing Data Protection and privacy issues is still emerging.	Continue to treat Data Protection as a key senior management issue, with further efforts to integrate it into IAD's Information Management strategy. Develop a comprehensive and integrated strategy and ensure that this is reviewed on a quarterly basis.
Staff Awareness	Some key staff appear to be unfamiliar with the Personal Information Policy. It should be noted that those same staff expressed enthusiasm to find out more once they were told of the problem. The complexity of policies, procedures and requirements presents a barrier to developing meaningful awareness.	The DSU7 team has started work on its programme of Data Protection awareness and training, and this will be reinforced by the Awareness and Audit project that has now commenced.
System Audit and Review	We were unable to obtain documentation or verbal evidence of any Data Protection audit or review process within IAD.	We reiterate that there is a need for a high level, structured and ongoing review both of management responsibilities, and of provisions for general oversight of information and data practices. The appointment of the DSU7 specialist team within IAD meets many of these requirements, but the work of this team should be regularly reviewed at the highest level of management. The new awareness and audit work will go a long way towards addressing this

		issue.
--	--	--------

Table 1: Summary of findings and recommendations

Documentation	The DWP and IAD documentation appears to be both comprehensive and largely complete - certainly when compared with our experience of Data Protection documentation in other large organisations. We believe that a full audit would conclude that the documentation is legally satisfactory and we have no hesitation in confirming its adequacy.	No action required.
Culture	We remain concerned about prospects for the ongoing quest for culture change in IAD. We believe that IAD's commitment to creating operational and management initiatives must be matched by an equally rigorous, systematic and embedded audit and evaluation process. From conversations with senior IAD staff we believe that substantial work still needs to be done at a behavioural and cultural level within the Directorate in order to achieve comprehensive excellence in data protection and security.	A comprehensive strategy should be devised to ensure that all opportunities to achieve culture change are fully exploited. Translating written procedures into appropriate action will be an ongoing challenge.

<p>Transparency</p>	<p>The Department's public profile - including press releases or the website - has yet to effectively publicise the work on the Longitudinal Study or provide meaningful details about related activities such as the Ethics Committee. This failure does not engender public trust, and has been the subject of lobby criticism¹.</p>	<p>As set out in our first stage report, any expectation of accountability and transparency must be reflected in the documentation published by DWP. This includes openness about processes and technical specifications. It can be argued that this level of transparency has not quite been achieved. This shortcoming presents a risk in terms of public relations. We draw attention in particular to the paucity of information on the IAD website with regard to the Longitudinal Study.</p>
---------------------	---	--

Table 1: Summary of findings and recommendations

¹ http://www.spy.org.uk/spyblog/archives/2004/06/where_is_the_dw.html

PART 3. ADEQUACY ASSESSMENT

Introduction This section describes the findings from our review of documents. Some of these have been developed for specific purposes by IAD; others are DWP-wide. Still more have been produced by other areas of government but have applicability to IAD.

Adequacy assessment of DWP documentation Although a small number of documents were either unavailable or incomplete at the time they were requested, it is clear that the DWP's published policies are extensive and generally sound. In our first stage report we made comments and recommendations relating to some key documents, but it is our judgement that overall the documentation will constitute a finding of Adequacy for data protection, and that the documentation is generally compliant with the Data Protection Act (1998).

Comments and recommendations relating to specific documents are contained in our Interim Report. However, the key indicators for Adequacy Assessment within the Directorate's Data Protection System parallel the findings of the Compliance Assessment in raising concerns over three key areas of procedures and operation:

- **Data Protection Strategy:** Whilst the necessary policies and standards are in place, there does not appear to be an overall strategy for implementing and managing Data Protection and Privacy issues;
- **Staff Awareness:** The IAD may fall short of its goal of excellence in terms of staff awareness of key policies. Some key staff, for example, appear to be unfamiliar with the Personal Information Policy. It should be noted that those same staff expressed enthusiasm to find out more once they were told of the problem, and that the issue is one of process and training, not of IAD staff motivation;
- **System Audit and Review:** We were unable to obtain documentation or verbal evidence of any Data Protection audit or review process within IAD.

We are satisfied that these issues will be adequately addressed by the new work on Data Protection awareness and audit.

We based our Adequacy findings and recommendations on a review of more than thirty documents and information sources. A full list of documents supplied to EPG is provided in **Appendix A**.

A list of documents that were requested but unavailable has also been provided in **Appendix A**. However, based on the strength of the documents provided, we are confident in awarding a finding of adequacy (a 'green light') to the documentation.

In light of the problems in obtaining all the requested documents, we recommend that in due course all relevant documents be brought together and indexed to provide a general resource for IAD and auditors. This collection should be regularly reviewed for relevance, compliance and accuracy.

PART 4. COMPLIANCE ASSESSMENT

Introduction This section documents our compliance assessment findings. The purposes of the pre-audit for compliance are to:

- ensure that the DWP is operating in accordance with its documented Policies, Codes of Practice, Guidelines and Procedures;
- indicate whether there are likely to be issues that will be raised when a full audit is conducted;
- establish parameters for excellence in data protection compliance.

Background The Compliance Audit is built on the findings of the Adequacy Audit, and is determined by a process of evidence gathering through staff interviews and observation. Much of this work is guided by the Information Commissioner's Data Protection Audit Manual, which sets out 240 questions relating to all aspects of Data Protection procedure. Our key task for this report was to systematically review answers to these 240 questions to determine an assessment.

The assessment The full list of questions is set out in **Appendix Two** of the **First Stage Report**. The area headings of the assessment in **Table 2** below correspond with the Appendix list, and we have colour coded each of them to provide an indication of where:

- evidence has yet to be discovered, or where we believe there are significant problems (**red**);
- where there is some indication of compliance (**amber**);
- where we are currently confident of full compliance (**green**).

Areas that do not appear to be relevant to IAD are highlighted in **blue**.

Table 2 shows the provisional assessment that we determined in July 2004 followed by the assessment that we have awarded IAD at 22nd December 2004. As with the audit overview in **Figure 1**, an improvement is clearly evident. We are pleased to note that all reds have moved to amber or green.

It is important to keep in mind that this list relates to application of the Departmental documentation. We should stress that the areas highlighted in red do not necessary indicate failure. These are primarily the aspects that will require greatest scrutiny in future Data Protection activities.

The compliance points listed in **Table 2** also form the privacy template for future compliance issues. These will be developed further as part of the awareness and audit work that has now commenced.

Ref.	Audit Area	Issue	Interim	Final	Reason for Change
A.1.1	The Data Protection System	Data Protection policy	Amber	Amber	
A.1.2		Staffing and reporting structures	Red	Green	The creation of the DSU7 team will resolve this.
A.1.3		Staff awareness and training	Red	Amber	Full documentation and the development of the DSU7 team have established the foundation for effective staff awareness. Implementation and full translation of the policies into staff practice is yet to emerge.
A.1.4 ²		System audit and review	Amber	Amber	
A.2.1	Documentation	Data protection procedures	Red	Green	Substantial improvement in staff development, lines of responsibility, documentation and oversight has created greater clarity and focus on data protection procedures.
A.2.2		Job descriptions and staff contracts	Green	Green	
A.2.3		Data collection	Green	Green	
A.3.1	Key business processes	Key business processes	Green	Green	
P.1.1	The First Data Protection Principle	Categories of personal data	Green	Green	
P.1.2		Schedule 2 - Grounds for legitimate processing of personal data	Red	Green	Clarified through legal advice.

Table 2: Preliminary compliance assessment

² A.1.4. 'Planning and Implementation' referenced in First Stage Report deemed unnecessary for Final Report

Ref.		Issue	Interim	Final	Reason for Change
P.1.3	The First Data Protection Principle (continued)	Schedule 3 - Grounds for legitimate processing of sensitive personal data	Red	Green	Clarified through legal advice.
P.1.4		Obtaining personal data	Red	Green	Clarified through legal advice. Full compliance subject to satisfaction of notification procedures in P.2.2.
P.1.5		Lawful processing	Red	Green	Clarified through legal advice.
P.1.6		Fair processing	Red	Green	Clarified through legal advice.
P.1.7		Exemptions from the first data protection principle	Red	Green	Clarified through legal advice.
P.2.1	The Second Data Protection Principle	Uses of personal data within the organisation	Green	Green	
P.2.2		Notification to the data subject	Red	Amber	While steps have been taken across IAD to improve notification procedures, questions still remain about the adequacy and effectiveness of the process. It may be necessary to conduct further work in this matter. This is particularly so in view of the specific circumstances relating to the IAD client base. To be lawful, notification must be intelligible and visible.
P.2.3		Notification to the Information Commissioner	Amber	Green	The Commissioner has been notified of all circumstances relating to areas covered by this report.

Table 2: Preliminary compliance assessment (continued)

Ref.	Audit Area	Issue	Interim	Final	Reason for Change
P.2.4	The Second Data Protection Principle (continued)	Use of existing personal data for new purposes	Red	Amber	Further information has been made available by IAD since the First Stage Report . A definitive statement from IAD's legal advisors on contractual arrangements with Data Processors (see T1.1 to T1.5) with regards to what third party processing, offshore processing and third party arrangements are possible (or precluded) is still required. Their assurance that the contract terms and parameters have been fully vetted and approved would permit this to move to a 'Green' rating.
P.2.5		Notification maintenance	Red	Green	Appropriate measures have been implemented to ensure that this condition is satisfied. It would however be advisable to request the legal department to provide an annual review of notification procedures to ensure that maintenance is adequate.
P.2.6		Disclosures of data	Red	Amber	Disclosures appear to be lawful. However we believe that contracts and arrangements should be systematically reviewed by the legal department to ensure consistency. This is particularly so with regard to the use of third parties in the processing of data disclosed for research purposes.
P.3.1	The Third Data Protection Principle	Adequacy and relevance of personal data	Amber	Green	Clarified through legal advice.
P.4.1	The Fourth Data Protection Principle	Accuracy of personal data	Green	Green	

P.4.2		Keeping personal data up-to-date	Green	Green	
-------	--	----------------------------------	-------	-------	--

Table 2: Preliminary compliance assessment (continued)

Ref.		Issue	Interim	Final	Reason for Change
P.5.1	The Fifth Data Protection Principle	Retention policy	Red	Amber	We recommend the development of a comprehensive retention policy reviewed annually to ensure that retention practices remain lawful. The policy should mandate relevant retention times depending upon the nature of the data and its use.
P.5.2		Review and deletion of personal data	Green	Green	
P.5.3		Deletion of personal data	Green	Green	
P.6.1	The Sixth Data Protection Principle	Subject access	Amber	Green	Documentation has now been provided. Procedures appear to be in order.
P.6.2		Appropriate withholding of personal data in response to a subject access request	Amber	Amber	
P.6.3		Processing that may cause damage or distress	Amber	Green	
P.6.4		Dealing with notices served by individuals	Red	Green	Documentation appears to be in order.
P.6.5		Automated decision taking	Red	Green	Staff interviews have satisfied us that this provision is adequate.
P.6.6		Rectification, blocking, erasure and destruction	Red	Green	Staff interviews have satisfied us that this provision is adequate.
P.6.7		Staff awareness	Red	Amber	Conditions as A.1.3 above. Implementation yet to be conducted.

Table 2: Preliminary compliance assessment (continued)

Ref.	Audit Area	Issue	Interim	Final	Reason for Change
P.7.1	The Seventh Data Protection Principle	Security policy	Amber	Green	Full documentation has now been sighted and appears to be in order. Appointment of DSU7 satisfies other requirements.
P.7.2		Unauthorised or unlawful processing of data	Red	Green	Clarified through legal advice.
P.7.3		Ensuring reliability of staff	Red	Amber	Awaiting full implementation of monitoring procedures and impact of procedures developed by DSU7.
P.7.4		Destruction of personal data	Green	Green	
P.7.5		Contingency planning - accidental loss, destruction, damage to personal data	Green	Green	
P.7.6		Contracts for processing carried out by third parties	N/A	N/A	
P.8.1		Adequate levels of protection	N/A	Amber	The use of third parties for processing of data requires clarification. Contract review by the legal department is essential.
P.8.2		Exempt transfers	N/A	Amber	As above.

Table 2: Preliminary compliance assessment (continued)

Ref.	Audit Area	Issue	Interim	Final	Reason for Change
T.1.1.1	Using Data Processors	Choosing a data processor	N/A	Amber	Further information has been made available by IAD since the First Stage Report . A definitive statement from IAD's legal advisors on contractual arrangements with Data Processors (see P2.4) with regards to what third party processing, offshore processing and third party arrangements are possible (or precluded) is still required. Their assurance that the contract terms and parameters have been fully vetted and approved would permit this to move to a 'Green' rating.
T.1.1.2		Contract initiation	N/A	Amber	As above.
T.1.1.3		Contract review	N/A	Amber	As above.
T.1.1.4		Contract modifications	N/A	Amber	As above.
T.1.1.5		Contract breaches	N/A	Amber	As above.
T.2.1	Notification	Notification to the Information Commissioner	N/A	Green	Subject to the satisfaction of above conditions.
T.2.2		Notification maintenance	N/A	Green	Subject to the satisfaction of above conditions.
T.3.1	Transitional Provisions	Processing already under way determined	Red	N/A	Appears not to be relevant to planned processing.
T.3.2		Dual regime	Red	N/A	Appears not to be relevant to planned processing.
T.3.3		The first and second transitional periods	Red	N/A	Appears not to be relevant to planned processing.

Table 2: Preliminary compliance assessment (continued)

Physical aspects

In our first stage report we drew attention to possible problems relating to the physical environment at Newcastle. These concerns resulted in part from issues arising from the open plan environment. They also stemmed from our successful efforts to socially engineer a means of bypassing security and entering protected premises at the site.

Since then we have been advised that a more secure location will be found for IAD staff affected by this issue (which, of course, is an issue that extends beyond IAD). This arrangement should substantially reduce security vulnerabilities at the site.

Similarly, staff could be more sensitive to threats to data under their control. A 'clear desk' policy may be difficult to implement, but in some circumstances it may be a necessary procedure. Computers should not display data unless the user is nearby. We understand that DSU7 is making an effort to rectify these shortcomings.

We understand that the sharing of passwords has been identified in the past as a potential issue. We anticipate that the new arrangements will go some way toward resolving this unfortunate problem.

Behaviour patterns

IAD has created a significant initiative in combating information misuse through the development of its 'Baby' system. Baby has been designed to detect suspicious behaviour in the use of personal data. The functionality is impressive. We would however suggest that IAD support further development of the programme to the point of more comprehensive integration in the audit process.

Ethics Committee

We would recommend that the important contribution of the Ethics Committee for the Longitudinal Study be promoted more widely. This will help inform and educate staff, while serving an important public function. The findings of the Committee could help raise staff awareness and thus improve the level of compliance. The IAD's website should be expanded to meet this requirement.

Appendix A. AUDIT SCHEDULE

**Documents
reviewed**

During the course of the review, the EPG team was provided with the following documents:

- Anti-virus Software Policy
- Data Matching Code of Practice - Work & Pensions Longitudinal Study
- Department of Social Security Code of Practice for Data Matching
- DWP document 'Computer Security & You'
- DWP Information Systems Security Standards
- DWP Internet Security Policy
- DWP Personal Information Policy
- DWP Security Awareness Presentation
- DWP Security Incidents Code for All Staff
- DWP Security Incidents Guide for Security Advisors
- Electronic Mail Security Policy
- Guidance to using the Work and Pensions Longitudinal Study - legal considerations
- Managers Guide to Security
- Material published on the DWP website, including material on the Longitudinal Study safeguards
- Newcastle & London view systems architecture charts
- Security Advisor's Handbook
- Social Security Fraud Act 2001 (s.3(1)) Code of Practice on Obtaining Information.

The following documentation was requested but could not be provided because of issues unrelated to the EPG review:

- Standards of Behaviour policies (we will attempt to view these on-site through the DWP Intranet)
- Risk assessments (prior and post system development) as specified in 5.2.1, 5.2.11, 6.8.2, 6.9.1, 7.7.14, 8.2.1, 8.3.8, 9.1.1, 10.7.1 and Annexe 1 of the DWP Information Systems Security Standards
- Any previous security reviews of DWP systems that have incorporated Data Protection (ie Part 10.5 of the ISSS) within their scope
- Relevant internal memos.

About the Enterprise Privacy Group

The Enterprise Privacy Group (EPG) is a membership body dedicated to creating innovative privacy management solutions. The EPG's team of experienced privacy professionals offers a unique and independent service for organisations that wish to set the highest possible standards for the handling of personal information.

Membership

The EPG offers a membership body that is open to commercial, government and academic organisations from around the world. EPG Members will benefit from meetings, workshops, reports, training courses, conferences and expert advice that will help them to minimise privacy-related risks in a highly cost-effective way.

Professional Services

The EPG's team of privacy professionals offer a broad spectrum of privacy services, including risk assessment, policy development, process implementation, training and awareness, data protection audits and recruitment of privacy officers on behalf of clients.

Enterprise Privacy Group

**Old Bank House
59 High Street
Odiham
Hants RG29 1LF
T: 01256 702325
F: 01256 702375**