
Highways Agency

Data Protection Audit Report

Final

Auditors:	Kai Winterbottom (Group Manager Good Practice) Claire Chadwick (Team Manager Audit) Chris Littler (Auditor)
Distribution:	
Draft Report:	Sian Jones (Data Protection Officer)
Final Report:	Graham Dalton (Chief Executive) Sian Jones (Data Protection Officer)
Date Issued:	7 July 2011

Contents

1. Background	page 2
2. Scope of the Audit	page 3
3. Audit Opinion	page 4
4. Summary of Audit Findings	page 5
5. Audit Approach	page 7
6. Audit Grading	page 8
7. Detailed Findings & Action Plan	page 9

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of the Highways Agency.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report; however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

1. Background

- 1.1 The Information Commissioner may, with the consent of the data controller, assess the extent to which good practice is applied when processing personal data and shall inform the data controller of the results of the assessment. (Data Protection Act (DPA) 1998 s51, (7))
- 1.2 The Information Commissioner sees auditing as a constructive process with real benefits for data controllers and so aims to establish, wherever possible, a participative approach. (Assessment Notice Code of Practice 2.1)
- 1.3 An Assessment Notice is the medium through which the Information Commissioner's Office (ICO) will seek to instigate a compulsory audit. However, the Assessment Notice Code of Practice, in the interests of clarity, distinguishes between compulsory and consensual audits. (Assessment Notices Code of Practice, 2.1, Para 6 & Appendix A.)

The Information Commissioner has reiterated a desire, in the first instance and as far as is practicable, to conduct consensual data protection audits.

- 1.4 The Highways Agency (HA) has agreed to a **consensual audit** by the ICO of its processing of personal data.

2. Scope of the Audit

- 2.1 Following pre-audit discussions with Sian Jones, Data Protection Officer (DPO), it was agreed that the audit would focus on the following areas:
- a. Data Protection Governance - The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the organisation.
 - b. Training and Awareness – The provision and monitoring of staff data protection training and the awareness of data protection requirements relating to their roles and responsibilities.
 - c. Records Management - The processes in place for managing both electronic and manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.
 - d. Security of Personal Data - The processes in place to ensure that there is adequate security over personal data.
 - e. Requests for personal data - The processes in place to respond to any requests for personal data. This will include requests by individuals for copies of their data (subject access requests) as well those made by third parties and sharing agreements.

3. Audit Opinion

- 3.1 The primary purpose of the audit is to provide the Information Commissioner and HA with an independent assurance of the extent to which HA, within the scope of this agreed audit is complying with the Data Protection Act 1998 (DPA).
- 3.2 The recommendations made are primarily around enhancing existing processes to facilitate compliance with the DPA.

Overall Conclusion	
Reasonable assurance	<p>The arrangements for data protection compliance with regard to governance and controls provide a reasonable assurance that processes and procedures are in place and being adhered to. The audit has identified some scope for improvement in existing arrangements and appropriate action is to be agreed to reduce the risk of non compliance.</p> <p>We have made five reasonable assurance assessments where controls could be enhanced to address the issues which are summarised below and presented fully in the 'detailed findings and action plan' section 7 of this report along with management responses.</p>

4. Summary of Audit Findings

4.1 Areas of Good Practice.

- The DPO, Agency Records Officer (ARO) and Electronic Records Officer all have well defined roles and responsibilities.
- There is a good staff awareness of the location of data protection related policies and procedures.
- The majority of staff have recently received data protection related training with refresher training planned.
- Where methods of data collection existed which may impact large numbers of individuals (such as CCTV and ANPR) appropriate explanations were provided within the Information Charter on the website.
- In reality, very little personal information is captured on CCTV and steps are taken to ensure that the amount of personal data collected is limited. (By camera infrastructure design, CCTV licensing and policies and RCC controls).
- Awareness of DP related concerns was high at the Regional Control Centres visited.
- The HA maintains close control of cameras to ensure that no inappropriate images are available to anyone that does not have an operational need to see them.
- The processes for the security and tracking of both manual and electronic records within the HA appear to be robust and well embedded.
- Staff were aware of the importance of reporting IT security incidents and there are clear procedures in place for their investigation.

4.2 Areas for Improvement.

- There are few measures in place by which the HA can actively monitor its compliance with the DPA and address identified risks and there is a lack of any forum to which data protection issues and risks can be escalated and addressed.
- Although policy states that personal data should not be downloaded onto portable media there are no physical prevention measures in place (i.e. endpoint control) or audit monitored trails to detect this.

- The HA confirm that all official laptops supplied by ATOS Origin, that could potentially hold personal data, are encrypted and identified on a central database. However it was reported that there were additional laptops in circulation at HA that are unencrypted which raises the risk of non compliance.
- The process for removal of system access for staff and contractors who leave HA should be reviewed and enforced.
- The current Email inbox capacity provides little incentive to appropriately use the SHARE system to save correspondence.
- There is currently little control over the weeding and retention of email correspondence.

5. Audit Approach

- 5.1 The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.
- 5.2 The ICO reviewed the processing of both staff and public personal data including but not limited to personnel records, the processing of any personal data captured from CCTV or ANPR cameras; Lands disposal, acquisitions and claims records, and locally held command and control logs.
- 5.3 The audit field work was undertaken on the 11 – 13 April 2011, at the following locations:
- Piccadilly Gate (Manchester)
 - Rob Lane Regional Control Centre (Warrington)
 - The Cube (Birmingham)
 - Quinton National Traffic Control Centre (Birmingham)
 - Quinton Regional Control Centre (Birmingham)
 - Lateral (Leeds)

6. Audit Grading

6.1 Audit reports are graded with an overall assurance opinion, and any issues and associated recommendations are classified individually to denote their relative importance, in accordance with the definitions in the table below.

Colour Code	Internal Audit Opinion	Recommendation Priority	Definitions
	High assurance	Minor points only are likely to be raised	The arrangements for data protection compliance with regard to governance and controls provide a high level of assurance that processes and procedures are in place and being adhered to. The audit has identified limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non compliance.
	Reasonable assurance	Low priority	The arrangements for data protection compliance with regard to governance and controls provide a reasonable assurance that processes and procedures are in place and being adhered to. The audit has identified some scope for improvement in existing arrangements.
	Limited assurance	Medium priority	The arrangements for data protection compliance with regard to governance and controls provide only limited assurance that processes and procedures are in place and are being adhered to. The audit has identified scope for improvement in existing arrangements
	Very Limited assurance	High priority	The arrangements for data protection compliance with regard to governance and controls provide very limited assurance that processes and procedures are in place and being adhered to. There is therefore a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.

7. Detailed Findings and Action Plan

Findings flowing from the audit will be risk categorised using the criteria defined in Section 6. The rating will take into account the impact of the risk and the probability that the risk will occur.

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
7.1 Data Protection Governance - The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the organisation.				
a.	Without a robust governance process for evaluating the effectiveness of data protection policies and procedures there is a risk that personal data may be processed inappropriately in contravention of the Data Protection Act 1998 resulting in regulatory action and/or reputational damage.	<p>A1. There is a data protection policy in place dated February 2006 which covers all areas of the DPA as part of larger Information Management Policy but there is no reference to lower level procedures.</p> <p>A2. There is a revised draft policy dated 8 December 2010 which has yet to be approved and disseminated to staff. This document refers to lower level procedures on PIAs, SARs and sharing however there is no mention of retention, fair processing or security (although these issues are covered in the 'data handling policy' and 'IT security guide'). There are no procedures in place to monitor compliance with the policy.</p> <p>A3. At the time of the visit there was not a permanent SIRO in place as the existing holder was due to leave the HA. There was no set time scale for the successor to be in post. There are</p>	<p>A2. It would be good practice to ensure that all areas of data protection are referred to; or other documentation signposted; within the overarching data protection policy. In addition to this it should include, where appropriate, provisions to monitor the HA's compliance with the policy.</p> <p>A3. The HA should ensure that a permanent SIRO is appointed in a timely manner and that they receive the necessary training for the role.</p>	<p>A2. Amendments to the policy will be made prior to its launch Responsible person: DPO Due Date: end July 11. Incorporating DP issues into the role of Information Manager's (IM) is currently under discussion enabling IMs to act as 'local champions' for DP issues providing greater scope to monitor compliance. Responsible person: ERM/DPO Due Date: Oct 2011 A3. A board-level SIRO has now been appointed.</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>IAO's at the HA but none were available for interview therefore an overview of the data protection knowledge of the SIRO and IAO's was not available.</p> <p>A4. There is a DPO whose role is to produce and maintain DP related policy, provide DP advice to staff and respond to any SARs. Their line manager is new to post and also line manages the IT security manager, records officer and electronic records officer, as a whole these staff form the information security policy and assurance team.</p> <p>A5. The key staff from the team contribute to a departmental Successes, Opportunities, Failures and Threats (SOFT) report on a monthly basis.</p> <p>A6. Whilst there are some management information produced by IT security and records management which demonstrates compliance with the DPA, these are not escalated to a single point and SAR statistics are not produced at all, therefore there is no clear corporate oversight of how the HA is complying with the DPA</p> <p>A7. The last Data Protection audit was carried out in April 2008 and there are</p>	<p>A6. Provide a more comprehensive and appropriate set of controls and measures (including for example SAR statistics, weeding / destruction logs and evidence of PIA use) to facilitate regular reporting of DPA compliance.</p> <p>A7. Include processes that could lead to non compliance with DPA</p>	<p>A6. Accepted in respect of SARs but other areas of compliance are reported via SOFT and Assurance reporting – SOFT reports are escalated to Directorate heads then to the Board. Assurance reports (IT security issues, data losses, DP breaches etc.) sent to Directorate heads and DfT who produce a cross-agencies report.</p> <p>We currently hold quarterly</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>no further audits planned. However the DPO has carried out small audits in specific areas such as CCTV and ANPR and there is currently an audit of the Security Policy Framework (SPF) ongoing.</p> <p>A8. There are risks relating to Data Protection in the HA risk register the majority of which relate to CCTV.</p> <p>A9. The use of PIAs is advocated for new systems which may be used to process personal data. However due to the spending review new systems are not being implemented at present.</p>	<p>98 as risks eligible for assessment in the risk register. This will raise the awareness within HA of the relevant issues and ensure that they are addressed at senior level and considered for inclusion in the internal audit plan.</p>	<p>security meetings with the Agency SIRO where areas of concern are raised and monitored.</p> <p>We are currently developing a risk based scorecard. This will provide a single point of management information across DP, RM, FOI and Security.</p> <p>We will be introducing PIAs, even if only at low level, into old systems as their RM-ADS are reviewed.</p> <p>Responsible person: VW Due Date: July 2011</p> <p>A7. We review and report our risk log of our information assets to DfT on a quarterly basis and provide an annual report to DfT (which is required by Cabinet Office) which is signed off by our SIRO, which reports on our information governance.</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
7.2 Training and Awareness - The provision and monitoring of staff data protection training and the awareness of data protection requirements relating to their roles and responsibilities.				
b.	<p>If staff do not receive appropriate data protection training, in accordance with their role, there is a risk that personal data will not be processed in accordance with the Data Protection Act 1998 resulting in regulatory action and reputational damage to the organisation.</p>	<p>B1. New starters have to complete an induction process which is supervised by their line manager. The line managers' induction check list ensures staff read relevant policies, including Data Protection, IT Security, Clear desk and email guide. There is no central log to show who has completed this and there is no evidence that this is actively monitored - it is down to individual line managers to ensure completion.</p> <p>B2. All staff are required to complete mandatory National School of Government online training, in their first week of induction. The Information Policy Officer has access to the National School of Government (NSG) database and is able to monitor take-up of this online training tool. Non compliance is escalated to line managers and then the Board. IAO's and SIRO's are required to complete the NSG levels 2 & 3 training.</p> <p>B3. The HA has issued new refresher training to complement previous NSG online training. This training, provided by the Dept of Transport, consists of two online videos to watch and a leaflet to read. There was concern amongst staff that the videos require audio,</p>	<p>B1. The HA should improve its oversight of data protection training and awareness by carrying out routine monitoring of who has received training and when. This can provide an important performance indicator for data protection compliance.</p> <p>B3. The HA should review the provision of training courses to ensure staff who handle personal data are trained accordingly. They should also implement a process to ensure that all appointed IAOs</p>	<p>B1. Line Managers currently complete a checklist for new starters which includes the NSG data handling/data protection training. It is not currently feasible to include this checklist in SSC but discussions are taking place to include the checklist in the new version of SSC. Responsible Person: SHARE Relationship Team Due Date: on-going discussions</p> <p>NSG have just released a new online training package which is mandatory and compliance monitoring tools are available. This package will be rolled out across the Agency over the next six to eight months.</p> <p>B3. Please see B1.</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>despite the fact many staff do not have access to headphones. In addition, monitoring of this refresher training is the responsibility of line managers. No central log or formal reporting structure is in place to monitor compliance.</p> <p>B4. The Acceptable Use Policy (AUP) has recently been introduced and although is not yet part of new starters' induction there has been a requirement since December 2010 for all staff to 'sign up' to this policy. This has been actively monitored and non compliance has resulted in users being locked out of their account. It was reported in March 2011 that less than 20 users had not signed the AUP policy.</p> <p>B5. All staff interviewed were aware of where to find data protection policies on the HA intranet. Updates to policies are notified through the 'Update' all staff email briefing.</p>	<p>and SIRO's complete annual training in information risk management, and annual refresher training thereafter, in line with Cabinet Office guidelines. All annual refresher training should be monitored and recorded with procedures in place to identify non compliance.</p> <p>B4. The HA should review the induction process to ensure all new staff complete the mandatory Cabinet Office 'Protecting Information' online training module. Monitoring of induction check lists will also ensure new staff have read the HA's relevant Information Security policies and procedures, including the Acceptable Use Policy, before handling any personal data.</p>	<p>B4. 2011/12 - DPO to undertake a programme of dp compliance reviews across business areas. The reviews will identify knowledge gaps and inform appropriate role-based training. The IPO receives a report detailing the IAOs for the business areas. The training is included within this report; the IPO sends reminders where training has not been completed.</p> <p>Confirm this is being carried out through review of starters' reports. Responsible Person: DPO Due Date: 2011/12</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
7.3 Records Management - The processes in place for managing both electronic and manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.				
c.	<p>In the absence of appropriate Records Management processes, there is a risk that records may not be processed in compliance with the Data Protection Act 1998, resulting in regulatory action by the Information Commissioner's Office, reputational damage to the data controller and/or damage and distress to individuals.</p>	<p>C1. The Agency Records Officer (ARO) is responsible for setting policy and procedures for managing information and reports directly to the Head of Information Security Policy and Assurance.</p> <p>The ARO works alongside the Electronic Records Manager (ERM) whose principle responsibility has been for policies and procedures in relation to SHARE, the Agency electronic documents records management system. The ARO is the key point of contact with the Departmental Records officer at the Department for Transport (DfT).</p> <p>C2. The HA identifies process owners in respect of reporting under its Stewardship Report. The ARO is a process owner and completes a risk assessment for each business area together with a summary.</p> <p>The Stewardship report is the main mechanism through which the Head of Information Security Policy and Assurance is provided with an assurance from her direct reports. This report is escalated through to the SIRO</p>		

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>who signs off on the assurance to the DfT.</p> <p>C3. HA has a high level records policy where the role of the ARO is clearly identified. The Records Management unit (RMU) handbook supports this high level policy with detailed procedures and guidance. Ownership of records management policies rests with the ARO.</p> <p>The RMU Handbook provided for review is out of date and refers to a previous incumbent of the ARO role. HA have reported that this will be included in a wider review of this area of work in the next six months.</p> <p>C4. Due to the way in which SHARE recognises a record, review dates for policies are not recorded on the document. The audit team were advised however that records management documents have been reviewed. It was unclear if any record is maintained to reflect this.</p> <p>C5. An Information asset register is held which should be reviewed and updated quarterly by each IAO. The register includes links to the risk assessments completed by each IAO on SHARE. The SIRO is responsible for the completion and return of the register to</p>	<p>C4. HA should ensure that review dates and revisions are appropriately recorded to provide an audit trail of policy development.</p> <p>C5. The Information Asset register should be regularly reviewed and updated by IAO's. The ICO recommends that HA implement a process through which the Head of Information Security receives a formal assurance that all</p>	<p>C4. Review dates were removed from new policies as unnecessary new records were being created upon a review just to update the review date when the policy itself had not changed. A review date will be included in the metadata in SHARE. RMU handbook will be updated by the new Physical Records Manager joining the team.</p> <p>Responsible Person: new Physical Records Manager Due Date: Oct 2011</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>the DfT and liaises with the Head of Information Security to ensure IAO's complete the return.</p> <p>It was reported that the process of updating the register may not have been as robust as is documented. However, the Head of Information Security Policy and Assurance is now taking a more active role in ensuring these are completed quarterly by IAO's.</p> <p>C6. The SHARE EDRM system is the HA records management system for electronic records. The RMU handbook clearly states that SHARE must be used. The ARO can in exceptional circumstances approve the use of shared drives where SHARE may not adequately support a team's work. (For example where large image files are frequently used).</p> <p>C7. The RMU is responsible for keeping up to date records of files and records using the IMPRES software to manage the ownership, location and retrieval of manual records.</p> <p>IMPRES is searchable and provides bar codes and basic reports. HA currently use Iron Mountain for archiving of its files and records and use IM Connect to facilitate retrieval. Records can</p>	<p>departments have appropriately considered and updated the information asset register.</p> <p>C7. HA should ensure that it has appropriate plans in place to ensure the migration of archiving from one supplier to another is handled securely and that appropriate contracts and assurances are implemented.</p>	<p>C5. A review of the HA Information Asset register is to be undertaken from the beginning of July 2011, where all directorates will be asked to review current and potential information assets for inclusions on the register. Further training and guidance on this will support the review process; much of this has been provided by DfT. A new reporting process is due to be launched by DfT which will mean that all IAO will be required to update risk registers on a DfT wide Information Asset Management System. Responsible Person: VW Due Date: HA Review concluding Sept 2011 – DfT roll out TBC (imminent)</p> <p>C7. A full audit of files as they transfer from Iron Mountain to TNT. A project plan is in-place and when it commences we will work with TNT to obtain statistics on the moves and results from the audit (ARO). The move is part of a wider</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>normally be retrieved within 24 hours.</p> <p>The tracking, retrieval and archiving process was well embedded and appeared to be well managed at the sites visited.</p> <p>C8. Where methods of data collection existed which may impact large numbers of individuals (such as CCTV and ANPR) appropriate explanations were provided within the Information Charter on the website.</p> <p>In reality, very little personal information is captured on CCTV and steps are taken to ensure that the amount of personal data collected is limited. (By camera infrastructure design, CCTV licensing and policies and RCC controls). Central to this is the reason for processing images; that they are necessary to support the key objectives of controlling the highways and managing incidents.</p> <p>C9. RCC's have a retention schedule for the records they keep and CCTV images are overwritten every 7 days. It was also reported that the quality of the image degrades approaching the 7 day cut off. Awareness of DP related concerns was high at the centres visited.</p>		<p>pan-government move lead by DCLG. We have received assurances from DCLG regarding secure handling and contract implementation.</p> <p>Responsible Person: ARO Due Date: Beginning Sept 2011</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>Traffic Officer control logs are kept to a minimum, personal data is normally confined to a name and contact number, this is consistent with the culture of only processing sufficient data to control the highways and manage incidents.</p> <p>C10. Contracts to share camera images are carefully controlled with access rights determining the quality of images that may be obtained from the HA. Images that are made publicly available are of the lowest quality and are 'still' images.</p> <p>The HA maintains close control of cameras using PTZ Blanking (pan, tilt zoom) to enable the blocking or blanking of images to ensure that no inappropriate images are available to anyone that does not have an operational need to see them.</p> <p>C11. The ARO and the ERM have implemented some measures to monitor records management performance, although to some extent this is a work in progress.</p> <p>The ERM is able to monitor the trends in volumes of files identified as records, utilization of folders, closure of SHARE accounts, utilization of intranet SHARE</p>		

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>guidance, Records Management inbox queries and group drive size trends.</p> <p>The effectiveness of some of these measures has yet to be fully evaluated, however the tracking currently being conducted by the ERM appears to show that the rate of files defined as records has slowed, whilst also showing a recent trend of increased use of team folders.</p> <p>C12. Group shared drives were locked down, are read only and can only be opened up with approval from the ARO. A 'non share ' folder on the 'Group' Drives for items not suitable for the EDRM. 'M' (Personal) drives can be used by staff but this is purged monthly, of everything created the previous month.</p> <p>SHARE folders are linked to specific retention periods based on the classes of information they should hold. Any files which have not been declared as records will be deleted at 2 years following the last edit.</p> <p>If records have been declared within a folder they will be deleted at the appropriate retention date for that folder.</p> <p>C13. It was less clear who is</p>	<p>C13. HA should identify what</p>	<p>C13. The Information Asset</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>responsible for the weeding and deletion of personal data contained on other applications such as HAL and HAIL and whether personal data on such systems is weeded in line with the retention schedules for SHARE. It was reported that records on HAL would be reviewed and deleted by the Information Policy Officer however this was not confirmed during the audit.</p> <p>C14. For HR casework (ie enquiries, grievance etc) a file is created in a locked HR folder within SHARE. Any grievance information is always kept separately from the main personnel file until a final decision made and then only the decision letter kept on the main file.</p> <p>In addition to the SHARE file all correspondence in relation to HR casework is kept within caseworkers email account, although there is intent to delete this when a case is closed there are no controls in place to ensure that this is done.</p> <p>C15. Further anecdotal feedback was provided which suggested that there is a cultural reliance within HA on MS Outlook in-boxes. Files within Outlook do not appear to be understood widely to be 'files or records' by staff, in the same way as Word or Excel documents.</p>	<p>personal data is stored within applications other than SHARE.</p> <p>HA should further ensure that retention schedules are implemented and that appropriate individuals with sufficient authority are responsible for ensuring personal data is weeded and deleted in accordance with the schedules.</p> <p>C15. HA should formally review its use of email internally, to establish the extent to which SHARE is used to appropriately save email correspondence.</p> <p>HA should consider a further</p>	<p>Register lists all HA information assets and whether or not they contain personal data. The DPOs compliance reviews will include assessments of retention and weeding schedules (see B3). Responsible Person: DPO Due Date: See above (2011/12)</p> <p>C15. A review of e-mail policy will be undertaken over the summer, and a 'de-tox your mailbox' programme rolled out early Autumn in advance of a reduction in mailbox limits. An investigation into reducing the</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>Previous attempts to reduce the size of Outlook in boxes (currently 2mb) did not receive high level support within HA. It is not good practice for personal data to be routinely kept within personal email accounts. Such information should be appropriately saved within SHARE.</p> <p>C16. During the audit it was reported that individual line managers kept manual paper records for their direct reports, such as a sickness records, back to work records, copies of medical certificates, copies of informal and formal warnings and long term absence reviews.</p> <p>It was unclear how long managers would retain personnel related documents. There was no formal procedure for ensuring such documents were returned to HR on termination of employment, destroyed in line with retention schedules or forwarded on to a new line manager.</p>	<p>promotion of SHARE for email files and in conjunction reduce the size of email inbox</p> <p>C16. Clear direction should be provided to Line Managers to ensure they are aware of what personal data they can retain locally for direct reports, for how long and how it should be secured. Clear procedures should be implemented for leavers and movers.</p>	<p>Mailbox limit slowly over several months will be carried out and a suitable mailbox limit agreed. Responsible Person: ARO Due Date: August 2011</p> <p>C16. DPO to liaise with HR to clarify procedures for line managers. Procedures will subsequently be re-enforced to line managers via HR. Responsible Person: DPO Due Date: July 2011</p>

Formatted: Font: Not Bold

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
7.4 Security of Personal Data - The processes in place to ensure that there is adequate security over personal data.				
d.	Without robust controls to ensure that personal data records, both manual and electronic, are held securely, there is a risk that they may be lost or used inappropriately, resulting in regulatory action against, and/or reputational damage to, the organisation, and damage or distress to individuals.	<p>D1. There is an IT Security Guide in place, which details the structures and controls in place to help secure the handling of personal data. However, there does not appear to be any integrated management oversight of risk and compliance arrangements at a senior level.</p> <p>D2. Other IT Security policies have not been reviewed recently (for example, the HA Removable Media policy) and it was not always clear, due to the absence of version control, if the documents provided were the most current version (for example, the Information Security Policy).</p> <p>D3. There was some evidence of spot checks and routine monitoring to test staff understanding and awareness of the clear desk policy.</p> <p>D4. Robust policies and procedures are in place with Iron Mountain, HA's 3rd party provider, for secure transportation and storage of manual records. Staff demonstrated a good knowledge of their responsibility in dealing with protectively marked documents and the need for secure storage of all manual records held on site.</p>	<p>D1 There is a risk that senior management do not have an oversight of IT security risks that may affect Data Protection compliance. The HA should review the reporting lines of the Information Security Policy and Assurance team to ensure compliance risks highlighted in the monthly SOFT report are monitored and reported to senior management, including the SIRO.</p> <p>D2. There is a risk that if policies and procedures are not reviewed on a regular basis that staff will not be aware of current legislation and Information Security practices. It is important that HA implement a consistent document control process for all policies and procedures, which clearly indicate ownership, review cycles and changes made.</p>	<p>D1. Review of reporting lines Responsible Person: VW Due Date: Sept 2011</p> <p>D2. The ARO will undertake a review of our document control process. Policy review to be included in policy team scorecard Responsible Person: ARO/VW Due Date: August 2011</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>D5. All offices visited had secure cupboards / rooms with good key control management and adequate physical security, including swipe card access to offices and front of house security. There was clear evidence, wherever possible, to adherence of a clear desk policy.</p> <p>D6. In HR it was stated that personal information was only sent via email if the receiving address was part of the Gsi network.</p> <p>D7. Information regarding occupational health issues is not sent via email as occupational health do not have Gsi email addresses, therefore everything is sent by mail or fax. If sending a fax the HR fax machine is always used and the recipient is called to tell them sending it and check received.</p> <p>D8. It was stated that a post log is in place for HR casework and any documentation containing personal information sent via the post is logged and then checked to ensure it has been received.</p> <p>D9. Atos Origin provides all network security, including firewalls and antivirus protection, which must conform to GSi and Cabinet Office</p>		

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>standards.</p> <p>D10. Network access to all HA's systems is controlled through Active Directory. Access to the network requires a complex password which users are forced to change quarterly.</p> <p>D11. Access to personnel records is role based ie each role is given an access ID code which stays with that role. When an employee moves job their role number will change, which will automatically change their access controls.</p> <p>D12. Correspondence Recording System (CRS) is role based and does not require a separate password.</p> <p>D13. RCC call recordings can only be accessed if the staff member has a have chip and pin card which only works within their own control area. Staff's access to systems is revoked as soon as they leave the organisation</p> <p>D14. The auditors were informed that CCTV footage is encrypted, and footage is usually taken from such a distance that vehicles and individuals would not be able to be identified. Following any manual intervention by an operator, cameras should return to their default position (either up or downstream). It</p>		

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>was stated that some newer cameras do not have this 'home' function.</p> <p>D15. A demonstration of the HA's Automatic Number Plate Recognition (ANPR) system clearly showed its only purpose is to produce intelligence about traffic flows.</p> <p>D16. Around 1,100 infra-red cameras are spread across 500 sites, The infrastructure is owned and operated by SERCO, under contract to the HA. A joint team from SERCO and the HA are responsible for the day to day operation of the system</p> <p>D17. The ANPR cameras record a 'brightness' scan of a vehicle registration number (VRN) which is then scrambled into a 'hash tag' Although the same VRN will always generate the same hash tag the process is not reversible - a VRN cannot be reconstructed from a hash tag. The hash tag is not unique – the same hash tag can be generated for up to 10 different vehicles.</p> <p>D18. HA does receive requests from the Police (approximately 40 per year) for help with enquiries. The Police would need to provide the VRN for HA to match a Hash tag, and will only do so where its is demonstrated that either life is in danger or an incident</p>		

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>involves a crime that carries a life sentence.</p> <p>HA are able to identify if that hash tag passed a particular camera at a particular time. The search always covers the whole country and therefore identical hash tags in different locations will be identified. Because more than one vehicle can have the same hash tag these searches cannot be used as evidence. The asset manager of the ANPR system receives monthly reports of searches conducted by SERCO.</p> <p>D19. HMG Security Policy Framework has a mandatory requirement (39e) that organisations have a lockdown policy to restrict unnecessary services and ensure that no user has more privileges (access and functionality) than required. Despite an IT Security Manager recommendation to the Board in 2010, HA have not mandated the implementation of an endpoint security solution to lockdown all desktop machines and laptops.</p> <p>D20. Although it is contrary to the Acceptable Use Policy and a disciplinary offence, the HA is relying on staff integrity to mitigate potential data loss. There is nothing to prevent personal data being downloaded to removable media and no robust monitoring of</p>	<p>D19. There is a risk that no endpoint security control combined with a reliance on staff to use removable media responsibly may result in a breach of the 7th data protection principle. Despite a recommendation to the Board in 2010 and it being a mandatory requirement of HMG's Security Policy Framework HA have chosen not to address this risk. It is important that the HA review this risk at senior level in the near future and consider routine monitoring of use of removable media.</p>	<p>D19. The risk has been reviewed at senior level; the decision was made to continue the security walkabouts across the HA office estate. A timetable for the walkabouts is currently being devised. Responsible Person: HP/VW Due Date: July 2011</p> <p>ICO Comment: The action proposed by the HA to this recommendation may not be sufficient to mitigate the identified risk. Our understanding is that security walkabouts rely on sight of unauthorised devices. End point control is a pro-active control. SPF</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>what is downloaded.</p> <p>D21. HA policy requires that only encrypted laptops and Ironkey USB drives may be used to store personal data.</p> <p>D22. Encrypted laptops and Ironkeys are issued by IT Service+ on receipt of an approved business case. IT Service+ requires all users to sign a declaration confirming they have read the security procedures and understand their responsibilities.</p> <p>D23. It was reported that Atos Origin do not provide a regular audit trail of attempted connections by non-approved devices.</p> <p>D24. No evidence was provided during the audit visit that all laptops have been encrypted to mitigate any risk relating to the accidental loss of personal data. However, it was reported that Atos Origin do hold this information and that all unencrypted laptops have had their network access disabled.</p> <p>D25. Information held on departmental laptops, Ironkeys and Blackberrys is encrypted to appropriate HMG standards.</p>	<p>D21. The HA should ensure any remaining laptops that potentially could be used to store personal data are encrypted by reviewing the laptop Asset Register and ensuring all non encrypted laptops have been returned.</p>	<p>Mandatory requirements 38 and 39 mandate more prescriptive controls than those proposed.</p> <p>D21. All laptops supplied by Atos Origin are encrypted. The laptop database, including the encryption key field, was clearly shown to the investigating officer. No further proof of laptop encryption was asked for.</p> <p>Responsible Person: Due Date:</p> <p>ICO Comment: D24 indicates that auditors were informed that there were unencrypted laptops in circulation at HA; if this is the case there remains a risk of unauthorised access to personal data and therefore a breach of the DPA.</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>D26. Atos Origin are able to monitor unauthorised use of non removable media through their anti virus software and one incident was reported in March 2011. However a random check of four HA Offices in autumn 2010 found unauthorised removable media in use in each office. It is not clear how robust the reporting and follow-up procedures for these type of incidents are.</p> <p>D27. Remote users can only access HA's network using a secure broadband connection. No access to the network is available through either wireless or 3G connection.</p> <p>D28. There is an HA Laptop / Blackberry Security Policy that details home and mobile workers' responsibilities in respect of the security of equipment and personal data. This must be signed before a laptop or Blackberry is issued.</p> <p>D29. HA insist on a home site visit before staff are allowed to work from home. It was reported there are controls in place to prevent remote workers from printing personal data at home without software installed by IT Assist and approved by the IT Security Department.</p>	<p>D28. There is a risk that staff who are allowed to print at home do not store and destroy documents securely. The HA must ensure that staff who have been given this facility are made aware of homeworking policies and procedures and that this is monitored.</p>	<p>D28. Review "working Securely away from the Office" and ensure all home workers are made aware of it. Responsible Person: ITSO Due Date: Dec 2011</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>D30. The robust roll-out of the Acceptable Use Policy exercise has left only 52 outstanding accounts who have not yet registered with the IT Security team. These include 35 Contractors accounts who may have left the HA. The exercise has also identified 125 users who had left the HA and 14 accounts that were not in Outlook.</p> <p>D31. The Accreditation Document Set for the HA's GSi connection was not reviewed. However, an ICO review of HA's internal audit of the Security Policy Framework found that the HA's IT logging and audit provisions do not comply with the GSi Code of Connection (CoCo) requirements for the HA's continued use of the GSI. The weakness was identified in the 2009 CESG CoCo review and an agreed target date for addressing this requirement was 31 December 2010. The audit review reports that this work has still not been completed.</p> <p>D32. Ensuring that third parties who process personal data on behalf of the HA (eg Shared Service Centre) have a contract that contains a clause in line with principle 7 of the DPA is the responsibility of procurement and the DPO or IT Security Manager are not involved in the process.</p>	<p>D30. There is a risk that staff and Contractors who leave the HA do not have their access rights to IT systems revoked. The roll out of the Acceptable Use Policy has identified staff who have left the HA and Contractors who may no longer require access. The IT Security team should monitor these anomalies to ensure staff and Contractors who have left the HA have their accounts removed from Active Directory.</p> <p>D32. It would be good practice for there to be oversight by the DPO, or other appropriate member of staff such as the SIRO, that principle 7 is being complied with in terms of third party data processors.</p>	<p>D30. The HR Policy Team published an article in the HA weekly newsletter Update on 30 June 2011 reminding all staff of the leavers process including the importance of following the 'Leavers Checklist' to revoke systems access – line managers to inform Atos; IT Security to be kept informed. Responsible Person: HR Policy Team; ATOS; IT Security Team Due Date: June 2011 – ongoing</p> <p>D32. DPO to liaise with Procurement to ensure principle 7 obligations are included within contracts. In addition to clauses in initial contract – additional checks should be carried out at regular intervals (such as renewal of</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>D33. Staff were aware of the importance of reporting any IT security incidents or loss of hardware. All incidents are recorded onto SHARE by the Security Liaison Officer through the online Security Incident report form. Details of these incidents are monitored and reported on in the monthly SOFT reports. Recent events have included a virus detected in a backup server in October 2010, malware on the Eastern RCC CCTV system in December 2010 and use of an unauthorised USB memory stick in BPR.</p> <p>D34. Any non IT related incidents such as loss or compromise of manual files containing personal data should be reported to the DPO, this is documented in the Security policy. There have been very few so they are not formally logged, but any incident would have a file detailing any investigation on SHARE. Incidents are also reported by HA DPO to the departmental DPO at DFT(c). To date there have been no reports to the ICO of any loss of personal data.</p>		<p>contract) Responsible Person: DPO Due Date: August 2011</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
7.5 Requests for personal data - The processes in place to respond to any requests for personal data. This will include requests by individuals for copies of their data (subject access requests) as well those made by third parties and sharing agreements.				
e.	<p>Without a robust process for responding to formal requests for personal data there is a risk of personal data being provided inappropriately in contravention of the Data Protection Act 1998 requirements resulting in regulatory action against the organisation and distress for individuals.</p>	<p>E1. There is a subject access policy in place which clearly describes how to identify a SAR and to forward to the DP advice team (which includes the DPO). This team process all staff SARs and any from the public. Any requests for CCTV footage or Command and Control logs are dealt with at the relevant regional control centre (RCC). Where requests are complex advice relating to disclosure/exemptions will be sought from the DPO.</p> <p>E2. Historically although a file is created for each SAR received a log showing when the SAR was received and when it was responded to has not been maintained. Since 1 April 2011 the DP advice team have used a SAR tracker which has the potential to produce statistics to evidence achieving statutory timescales, however due to the infancy of this project this was yet to be done at the time of the audit.</p> <p>E3. Requests made to RCC's are logged on CRS and should be responded to within 15 working days in line with HA's normal service level agreements.</p> <p>E4. SAR statistics are not escalated at</p>	<p>E4. Ensure that the SAR tracker is</p>	<p>E4. The Tracker is currently</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>present to evidence compliance. The DP advice team do contribute to a departmental 'Soft' report and any SARs exceeding 40 days should be highlighted as a 'failure', however this does not provide an overall picture of how SARs are being dealt with within the HA.</p> <p>E5. Staff who carry out redaction on SARs have received appropriate training on the exemptions to the DPA and what can be redacted. However there is no monitoring carried out to ensure that the exemptions are being applied consistently.</p> <p>E6. Copies of the original file are retained on the 'SHARE' (record management system) in an area only accessible to relevant staff so it can be referred to if a query on the redacted information is received.</p> <p>E7. The majority of third party requests are received from the police, with which there are sharing protocols in place. The police are required to complete a P1 form giving details of the incident/footage they require.</p> <p>E8. The DPO has the opportunity to review all data sharing protocols to ensure they contain the correct clauses. A copy of each protocol</p>	<p>used to produce statistics that demonstrate HA compliance with principle 6 of DPA and they are escalated to the appropriate forum.</p> <p>E5. It would be good practice to carry out monitoring on a random sample of SAR responses to ensure that exemptions and any resulting redaction are being carried out in a manner consistent with HA policy and the DPA.</p> <p>E8. It would be good practice for the DPO to review of any protocol when significant amendments are made.</p>	<p>being used to identify SAR patterns and compliance issues across the business. Areas of non-compliance will continue to be appropriately escalated (via monthly SOFT Reports or immediate reporting if there is a significant breach/risk).</p> <p>E5. DPO to raise issue of dip-sampling of SAR responses with DfT (and other Executive Agencies) to ensure a consistent cross-agency approach. Responsible Person: DPO Due Date: August 2011</p> <p>E8 & E9: Protocols currently contain review dates. In conjunction with business areas DPO to implement procedures</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>together with any correspondence with its creator is retained by the DPO on 'SHARE' so that it can be referred to if necessary.</p> <p>E9. There is no formal monitoring of data sharing protocols once they are in place by the DPO; this is dealt with by the department who created the protocol.</p>	<p>E9. Monitoring; either by the relevant department or DPO; of data sharing to ensure it is being carried out in line with the relevant protocol would demonstrate good practice.</p>	<p>whereby significant amendments to protocols will be reviewed by DPO. This process will incorporate compliance monitoring by all parties to the protocols. Responsible Person: DPO Due Date: October 2011</p>

The agreed actions may be subject to a follow up audit to establish whether they have been implemented.

7.6 Any queries regarding this report should be directed to Claire Chadwick, ICO Audit.

7.7 During our audit, all the employees that we interviewed were helpful and co-operative. This assisted the audit team in developing an understanding of the selected agencies' and establishments' working practices, policies and procedures. The following staff members were particularly helpful in organising the audit:

Sian Jones, Data Protection Officer