Good Practice

Audit outcomes analysis

Local Authorities – January 2011 to December 2012

This report is based on the final audit reports the ICO completed in the local government sector during the above period. No individual organisation is named in the report.

Assurance ratings

When conducting an audit, we assess the arrangements an organisation has in place for complying with the Data Protection Act 1998 (DPA) and the extent to which they are being adhered to.

We then give an overall 'assurance rating' (as described below) indicating the extent to which controls are in place and are effective.

Assurance rating	Description
High assurance	Limited scope for improving existing arrangements. Significant action unlikely to be required.
Reasonable assurance	Some scope for improvement in existing arrangements.
Limited assurance	Scope for improvement in existing arrangements
Very limited assurance	Substantial risk of non compliance with DPA. Immediate action required.

Overall audit assurance ratings

During the period, we audited 32 local authorities and gave the following assurance ratings.

Year	Audits completed	High assurance	Reasonable assurance	Limited assurance	Very limited assurance
2011	11	0	3	7	1
2012	21	2	9	10	0

- Over both years, 38% fell within the reasonable assurance range and 53% fell within the limited assurance range.
- There has been a 16% increase in the number of reasonable assurance ratings achieved year on year.
- There has been a 16% decrease in the number of limited assurance ratings achieved year on year.
- Two local authorities have been identified as having a high level of assurance during 2012.

Scope area assurance ratings

ICO audits can cover a number of key scope areas (described below). We give an assurance level of the overall performance in each scope area. During the period, we gave the following assurance ratings.

Scope area	Rating	Total
DP Governance The arrangements and controls in place to ensure compliance with the DPA.	High	1
	Reasonable	5
	Limited	12
	Very limited	1
Records management The processes in place for managing both electronic and manual records containing personal data.	High	0
	Reasonable	11
	Limited	13
	Very limited	0
Requests for personal data The procedures in place to deal with any requests for personal data.	High	4
	Reasonable	8
	Limited	10
	Very limited	1
Security of personal data The technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form.	High	2
	Reasonable	14
	Limited	8
	Very limited	0
Training and awareness The provision and monitoring of staff DPA training and the awareness of DPA requirements relating to their roles and responsibilities.	High	1
	Reasonable	6
	Limited	6
	Very limited	0
Freedom of information requests The arrangements and controls in place to ensure compliance with the FOI Act.	High	0
	Reasonable	2
	Limited	0
	Very limited	1

Common areas of good practice

We observed good practice in **security of personal data** and **requests for personal data.** In particular;

- embedding of incident security management policies;
- reporting on compliance with the statutory timeframes for responding to subject access requests; and
- implementation of a structured information security framework and policies.

Common areas for improvement

A common area for improvement is **governance**. In particular;

- inconsistent information risk management;
- absence of effective DP compliance monitoring; and
- lack of privacy impact assessments for either new projects or significant changes to existing systems.

General findings and observations

The following areas of control were typically observed across the sector:

- ✓ Internal Audit data protection activities and action plans in place.
- ✓ Staff awareness of the security incident/breach notification process.
- ✓ Policies and procedures in place and available to all staff. Employees understand and can refer to their responsibilities under the DPA.
- ✓ Controls implemented to secure personal data, for example policies and network access controls, had been developed and reviewed.
- ✓ Measures to ensure encryption for all mobile devices used by employees.
- ✓ Staff forums in place to feedback data protection issues and risks.
- ✓ Fair processing notification published to ensure that the public know how and when the authority will process their personal data.
- ✓ Accountability assigned for the processing of all subject access requests received.
- ✓ Information governance roles and responsibilities assigned at Board level.

Detailed findings and observations - good practice

- ✓ An un-redacted and redacted version of personal data compiled in response to subject access requests is retained which provides a complete audit trail and will assist in answering any redaction related enquiries.
- ✓ The adoption of the new SASPI Scottish protocol (based on WASPI) for new data sharing agreements.
- ✓ Training resources shared between London Boroughs through an e-learning portal as an effective and efficient way to ensure all staff receive relevant training.
- ✓ Data protection training completion rates feed into annual staff appraisals and are included in performance objectives for all employees.
- ✓ Local working groups set up to share experiences and best practice amongst group members. These were generally groups consisting of representatives from other public sector organisations.

- ✓ An embedded clear desk culture in place, which includes the use of the 'Think Privacy' awareness posters available from the ICO website.

- ✓ Internal audit conduct annual assurance reviews of data protection and information governance. These reviews have been designed around the "Local Public Services Data Handling Guidelines" (August 2012).

- ✓ The data protection e-learning training course includes a 'test' at the end for which there is a required 85% pass mark, providing an assurance of a candidate's understanding following completion of the course.

- ✓ Data quality reviews of social care files are conducted by peers in differing London Boroughs, thereby ensuring objectivity and sharing best practice.

- ✓ Experienced, pro-active Information Governance Manager available for consultation and advice from any area of the organisation, with direct reporting lines to senior management.

- ✓ Information security metrics produced in a quarterly 'Organisational Health Report' and viewed at executive level - metrics including data loss incidents, training achievement compliance, excessive web and email usage and SAR/FoI compliance.

- ✓ All employees are required to electronically confirm they have read and understood the Council's Information Security policy every 90 days. If users fail to provide confirmation after five log ins their network access is revoked and their line manager is notified.

Detailed findings and observations - for consideration

Overall controls could be enhanced with the introduction or development of the following:

- The use of regular and enhanced compliance monitoring and reporting, in particular to Board level, to provide executive oversight and understanding of performance and to gain the support necessary to drive improvements.

- Formal systems to record and manage any information related risks such as risk registers and information asset registers.

- An embedded Risk Management Policy which includes information risk management, that sets out how the organisation and its data processors manage information risk, and how compliance with the policy is monitored.

- Assignment of senior named Information Asset Owners (IAO's) to each information asset that processes personal data. Continual risk assessment on a periodic basis of information assets.

- A record or log of the manual records held by individual departments and effective sign in/out procedure for instances where a paper record is taken for homeworking.

- The implementation of a robust Mover / Role Transfer policy to ensure employees with access to applications or systems containing sensitive data have had their access rights revoked or adjusted when changing departments.

- Delivery of refresher data protection training through a continuous DP training strategy which is communicated to all employees and monitored to ensure target completion dates are achieved.

- Roll out of a programme of specialised data protection training for key information governance roles within the organisation, e.g. records management roles, DPO, IAO, SIRO.

- Creation of a log of which exemptions have been applied to individual requests for personal information to ensure complete records of legislative considerations that have been taken into account in each case.

Feedback survey results summary

Feedback is important as it helps us to improve. After an audit we write to the organisation concerned to ask for feedback on the audit process and their experience of the audit.

From the surveys returned for the period, we received the following comments.

- ✓ The audit by the ICO helped to bring the DPA to the forefront of the Council's agenda especially in these challenging times within the public sector.

- ✓ The audit provided a focus and structure to the Council's programme of reviewing its performance in relation to data protection and information security. I believe that the audit has enabled change to occur more quickly than it may have otherwise done and there is a clear action plan for the Council to follow over the coming months.

- ✓ It would be helpful if there was a clear message about who the ICO expect to be present from the Council at the introductory meeting. There was also uncertainty prior to the audit about how outstanding complaints or self-referrals to the ICO regarding data breaches would be considered as part of the audit.

- ✓ The audit has served three purposes: (1) confirmed that the resources, training, systems and controls we have implemented will help to secure the data that we process; (2) helped to identify gaps and weakness and (3) raised the profile of the ICO and data protection throughout the organisation.