Good Practice

Audit outcomes analysis

Private Sector – January 2011 to December 2012

This report is based on the final audit reports the ICO completed in the private 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 21 private sector organisations and gave the following assurance ratings.

Year	Audits completed	High assurance	Reasonable assurance	Limited assurance	Very limited assurance
2011 & 2012	21	13	7	1	0

- Over the two years, 62% achieved a high assurance rating
- 33% fell within the reasonable assurance range.
- There have been no very limited assurance ratings issued during the period.

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	9
	Reasonable	7
	Limited	1
	Very limited	0
Records management The processes in place for managing both electronic and manual records containing personal data.	High	2
	Reasonable	8
	Limited	2
	Very limited	0
Requests for personal data The procedures in place to deal with any requests for personal data.	High	6
	Reasonable	4
	Limited	1
	Very limited	0
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	9
	Reasonable	5
	Limited	0
	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	10
	Reasonable	3
	Limited	0
	Very limited	0

Common areas of good practice

We observed good practice in all scope areas, in particular **governance, training and awareness** and **security of personal data**, as a result of;

- the existence, periodic review and active compliance monitoring of data protection policies and procedures, which were made available to all staff;
- implementation of a structured information security framework and policies including incident reporting procedures; and
- data protection and information security training programmes.

Common areas for improvement

A common area for improvement is **records management**. This is frequently attributed to;

- lack of controls or process for disposal of electronic and / or manual records; and
- the absence of effective controls to log and track the secure movement of manual records.

Detailed findings and observations - good practice

The following areas of good practice were observed:

- ✓ Floors / offices have designated working areas where personal devices are not permitted, reducing the risk of unauthorised copying of information. Lockers are provided in which to store personal devices such as mobile phones and specific authorisation is required before devices are permitted into restricted areas.

- ✓ Annual internal audit plan in place that assesses data protection practices against the ICO Audit Manual. Control self-assessment and compliance testing is completed on a quarterly basis at business unit level against key business processes and information security.

- ✓ Business Continuity Plan implemented, which includes incident management that is tested periodically to ensure it remains fit for purpose.

- ✓ Data protection representatives have been nominated in each business unit. It is their responsibility to identify data protection issues within their departments, complete the 'breach and issues' log and report back to senior management. Representatives must also complete departmental DPA compliance checks at least once a month and report back to management.

- ✓ A system / tool is used to track all IP-addressable hardware (including PCs, laptops and printers) and software across the organisation. This automatically identifies new hardware and software on the network and adds it to the IT asset database.

- ✓ All data processor contracts are monitored annually by Procurement. The monitoring focuses on high risk arrangements. Most contracts will have standard data protection / security clauses but any contracts posing new or unique data protection issues would be reviewed by the DPO before being rolled out. Any high risk projects involving a data processor would require information security management input as standard.

- ✓ The DPA e-learning module automatically 'expires' after 12 months and is subsequently reviewed by the DPO, who has 30 days to review and update the module. The module also holds the functionality to be updated throughout the year should this be deemed necessary, for instance in response to changes in the law or corporate policies.

- ✓ Training programmes are reviewed to take account of lessons learned / training evaluation, trend analysis and information uncovered during compliance monitoring and breach reporting, sector specific issues emerging and new software tools / technological developments.

- ✓ Testing of the incident management process takes place through the use of simulations. These can run over several days, incorporate staff from across the business, and are used to test complex incidents. Although the participants are told they will be involved in a simulation, they are not given any details of the scenario.

Detailed findings and observations - for consideration

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

- Privacy impact assessments for new (or significant changes to) information systems and data handling processes to identify and address information risks in the early stages of a project.

- Refinement of existing controls for tracking of manual records in storage and subsequent destruction to support retention monitoring.

- A disposal or retention schedule and supporting processes to ensure electronic records are not kept for longer than necessary.

- Reporting mechanisms through to senior management to track and monitor performance towards achieving the statutory timeframe for responses to subject access requests.

- Tighter controls implemented in relation to user access to information systems, for example role based access rights, and a robust starters / movers / leavers procedure.

- Data protection and information security training delivered as part of the induction programme prior to access being granted to systems processing personal data.

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.

- ✓ Data protection has always been very important here. The audit process and resultant report helped raise its profile further. We have discussed it with senior people and included a summary in our Group Audit Committee update. We have distributed the executive summary to a wide audience and it has given us the chance to discuss DP with new areas. All in all, it was a very worthwhile exercise for us.

- ✓ The ICO audit provided a welcome independent assessment of our DP compliance. It helped reinforce the importance of data protection and it has provided us with a level of assurance associated with effective DP governance, training & awareness and record management.

- ✓ We agreed a scope based on three audit themes and a 'slice' through our business. The reports only referred to the three themes. It didn't have a material impact but it meant that we had more explaining to do! It was a very positive experience for us and I hope it was for you too.