

Data Protection in 2010

Workshop B - Data protection auditing

Outcomes

Audit programme

The ICO decides which organisations to audit by using a risk-based approach, including factors such as complaints history, previous enforcement action, and corporate and media reports. The key consideration is always the likely impact on the individual in terms of privacy impact. It was questioned as to whether the ICO held an 'intelligence database' but CT confirmed it is simply a knowledge base where accuracy and reliability of information is key, and information weighted accordingly – for example complaints where the assessment is 'compliance likely' are not going to be heavily weighted.

A consensual audit will always be sought initially, for both public and private sector organisations. Some organisations volunteer for audit.

Audit – engagement planning

The process was discussed, including the initial contact letter, scoping, the letter of engagement and detailed schedules. It was questioned whether any organisations have ever refused an audit, and confirmed that they had not, but if they did the ICO would record that help had been offered but declined.

Audit – adequacy audit

This is a desk-based exercise carried out at the ICO offices, where organisational policies, processes and procedures, governance, and training materials are examined for general compliance, completeness, user-friendliness and regular reviews.

Audit – compliance audit

This is conducted on the organisation's site, and lasts anything between half a day and 7-8 days – although 3 days is an average. Staff meetings are held, preferably at their desks. Meetings and

evidence gathering vary in emphasis depending on the scope of the audit, which could be data protection awareness, business procedures, security for example.

Audit – reports

These have changed significantly over the past few years after feedback and external advice has been taken into account. The report includes an overall opinion on current levels of compliance, a summary of areas of good practice and areas for improvement found, and detailed findings and recommendations

Audit report cycle / follow-up

The ICO sends a draft report for accuracy review by the organisation. Once approved by the organisation, a final version is sent to the CEO, with organisational comments as appropriate. Publication of audit reports was discussed, and CT confirmed that as a general rule we would not publish consensual audits as this would be detrimental to the relationship. The ICO's legal power to publish was questioned – the ICO has no explicit legal power to publish but an implicit power exists. Under the Freedom of Information Act (FOIA) we may be required to disclose a report, although the organisation would be approached before any such disclosure. Any commercially sensitive or security issues would not be published.

Follow-up may include requesting written confirmation from the organisation that a minor recommendation has been actioned, or a follow-up visit may be appropriate to assess specific areas.

It was confirmed that the ICO will not fine an organisation as a result of an audit, and it is highly unlikely that enforcement action would be taken as a result of an audit – unless specific issues remained unaddressed after a follow-up visit, for example.

Audit assessment notices

This comes into force in April 2010 and will allow the ICO to carry out compulsory as well as consensual audits. A code of practice is out for consultation at the moment.

A key point is that the ICO intends to follow the consensual route wherever possible, unless an organisation declined an audit and we felt an audit was absolutely necessary.

Compulsory audits can be carried out on government departments and public authorities as defined by the FOIA. Other bodies (which

could be private sector) could be compulsorily audited by Order of the Secretary of State, after representations made by the Information Commissioner. This would usually be when there were sectoral issues, not those of individual companies.

Assessment notices and reports may be published in summary form.

ICO audit goals and objectives

The ICO see audits as an educational tool to help deliver compliance by organisations, and is to increase the volume of audits undertaken. The intention is to speed up the audit process, and make them more risk-focused.

Audit – organisational benefits

Audits provide many benefits to organisations – identifying risks, providing assurance that processes are compliant, and increasing awareness across the levels of the organisation are just some.