

Achieving our value of being a model of best practice

ico.

Information Commissioner's Office

1. The Value

A model of best practice

We do not ask others to do what we are not prepared to do ourselves.

“As a model of best practice, ensure we have the right systems and resources in place to enable us to comply efficiently with information rights legislation.”

Corporate Plan 2010-2013

The ICO’s mission, vision and values have set the overall direction for ICO as it moves through a period of rapid change. The internal compliance and information security strategy is a clear statement of ICO’s commitment to compliance with information rights legislation.

This strategy takes account of, and supports ICO’s operational objectives. It ensures that a balance is struck between operational and compliance objectives, a balance that is reflected in the targets which have been set.

Compliance activity will not happen in isolation, it must be fully integrated with all of ICO’s operational and support functions.

2. The context

The context within which ICO operates is unusual. Subject to the laws for which it is responsible, it is in effect its own regulator. ICO must ensure legal and regulatory compliance and achieve best practice.

The legal and regulatory framework is outlined below.

The legislation regulated by ICO

- The Data Protection Act 1998
- The Freedom of Information Act 2000
- The Environmental Information Regulations 2004
- Privacy and Electronic Communications Regulations 2003

Other related legislation

- The Public Records Act 1958
- The Re-Use of Public Sector Information Regulations 2005

Related guidance and codes of good practice

- Security Policy Framework (Cabinet Office)
- Government Secure Intranet (GSI) Code of Connection
- Government led initiatives relating to information security eg the data handling review
- ICO's published guidance

3. Role of the Internal Compliance Department

The internal compliance department exists to ensure that we not only comply with legal and regulatory requirements but also, achieve best practice.

The Head of Internal Compliance will have primary responsibility for delivery in accordance with this strategy. She will do this through the work of 3 teams.

1. Information Access (IA)

Activities which relate to the handling of information requests and the proactive publication of information.

2. Awareness and Monitoring (AM)

Activities to make sure that staff and suppliers are aware of, and understand ICO's information handling and security policies. Regular monitoring to ensure compliance with ICO's internal policies and published codes of practice and guidance. Implementing recommendations derived from monitoring exercises.

3. Continuous Improvement and Development (CID)

Identifying, prioritising and focusing on areas for improvement and ensuring new systems or processes are compliance ready.

4. The Strategy

The remaining sections of this document describe eight strategic aims designed to ensure ICO's legal compliance and achieve best practice. It describes how those aims will be delivered (tactics), the timescales and indicators for success.

Key	
ST	Short Term (2010-11)
MT	Medium Term (2011-12)
LT	Long Term (2012-13)

To be a Model of Best Practice

Information Access

Strategic Aim (1) - To ensure information requests are handled effectively, efficiently, consistently and within the statutory timescales.

Tactics:

- Continue to develop the skills and expertise of the information access team to ensure high quality, timely and consistent responses to information requests.(ST-LT)
- Review the information request handling procedures looking for opportunities to improve efficiency.(ST)
- Introduce procedures for quality checking.(ST)
- Improve the internal review handling procedure ensuring that lessons are learnt from reviews and reducing the elapsed time for completion of reviews.(ST)
- Working with the business areas look for ways to ensure information requests are identified promptly and responded to within the statutory timescales.(ST-MT)
- Working closely with Policy Delivery ensure that existing and new external guidance relating to the handling of information requests is incorporated into information request handling.(ST-LT)
- Improve the internal reporting on information request handling providing additional information about the subject matter of requests and compliance with the statutory timescales.(ST-LT)
- Publish our information request handling procedures and statistics to improve transparency about information access.(ST)

Indicators of Success

1. ICO does not meet the monitoring and enforcement trigger points for S10 of FOIA.
2. 95% of information requests are handled within the statutory timescales (ICO performance will be published by the Ministry of Justice).
3. 95% of internal reviews handled within 20 days.
4. Ensure monthly information request and internal review statistics are published on ICO's website.

To Be a Model of Best Practice

Information Access

Strategic Aim (2) – To develop ICO’s proactive publication of information.

Tactics:

- Analyse the subject of information requests made to ICO and consider whether the information requested could be added to the Publication Scheme.(ST-LT)
- Review and update the Publication Scheme.(ST-LT)
- Implement procedures to ensure the Publication Scheme is updated on a regular basis.(ST)
- Be alert to activities and events around ICO, anticipating possible information requests and proactively publishing information.(ST-LT)
- Relaunch the disclosure log and keep updated with cases which fulfil the disclosure log criteria.(ST)
- Review ICO’s Notification and ensure that it is up to date.(ST-LT)
- Increase transparency about ICO’s own compliance with the development of pages on the corporate website ‘How we comply with the legislation which we regulate.’ (ST)
- Embed the culture of proactive publication throughout ICO. (ST-MT)
- To ensure alignment with government commitments to openness and proactive release of information (ST-LT).

Indicators of Success

1. Reduction in the number of information requests being received through the proactive publication of information releasing resource for other activities.
2. Demonstrating good practice externally with an effective and up to date Publication Scheme and disclosure log.
3. Reducing the number of enquiries about our compliance through increased transparency.

To Be a Model of Best Practice

Internal Compliance and Information Security Awareness

Strategic Aim (3) – To improve and maintain at a consistently high level staff and supplier awareness of ICO's information handling and security policies.

Tactics:

- Development and implementation of a rolling programme of awareness activity using a variety of methods to increase internal compliance awareness.(ST-LT)
- Improvements to the information provided to new staff , new suppliers and during the induction process.(ST)
- Implementation of regular and effective refresher training for staff and suppliers.(ST-MT)
- Development of ICON so that clear and up to date information is easily accessible to all staff.(ST-LT)
- Development of a single point of contact facility for all staff for all queries relating to internal compliance.(ST)
- Development of a single point of contact facility for the regional offices ensuring that all compliance messages are conveyed and issues specific to the regional offices are addressed.(ST)
- Ensure that where internal compliance incidents occur, lessons are learnt and recommendations implemented. (ST-LT)
- Promotion of Meridio as the corporate file store for ICO's electronic records.(ST-LT)

Indicators of Success

1. Internal compliance incidents do not occur which would have been prevented if staff or suppliers had been aware of a policy or procedure.
2. Staff know who to go to for advice and this is provided in a timely manner.
3. Monitoring exercises demonstrate compliance and high awareness.
4. Staff survey questions reveal a high level of internal compliance awareness.

To Be a Model of Best Practice

Internal Compliance and Information Security – Monitoring

Strategic Aim (4) – Regular monitoring to ensure compliance with internal policies and procedures and with the guidance and codes of practice published externally.

Tactics:

- Develop a rolling programme to monitor ICO's compliance with internal compliance policies and procedures and compliance with the codes of practice and guidance it has published externally eg the employment code of practice.(ST-LT)
- Report on monitoring and take prompt action to address any recommendations.(ST-LT)
- Ensure DP and FOI provisions are included in new and existing third party contracts and ensure compliance with those contractual responsibilities is audited.(ST-LT)

Indicators of success:

1. Internal compliance incidents do not occur as a result of a breach of an ICO policy or non compliance with guidance or codes of practice published externally.
2. Evidence that awareness activity is effective by reducing the number of recommendations after each monitoring exercise.

To Be a Model of Best Practice

Embedding compliance within ICO processes – continuous improvement and development

Strategic Aim (5) – Continue to embed records management best practice across ICO ensuring compliance with S46 of FOIA and the data protection principles.

Tactics

- Ensure we know what records we hold, in what format they are held and their location through the continued development and maintenance of an information asset register.(ST)
- Complete the risk assessment on ICO's information assets and ensure appropriate controls are in place.(ST)
- Finalise the corporate retention and disposal schedule for ICO records and develop processes to identify and dispose of any expired records.(ST-MT)
- Continue to develop processes for the effective management of legacy paper files.(ST)
- Continue to embed records management procedures.(ST-LT)

Indicators for success

1. An up to date information asset register.
2. Quicker access to information assets, reducing information risk and the time required to respond to information requests.
3. A positive outcome to self assessment under the Section 46 Code – using The National Archives methodology.
4. Public records worthy of preservation identified and managed accordingly.
5. Well managed explicit information providing a solid basis for the development and implementation of knowledge management practice across the ICO.
6. Disposal of records routinely happening in accordance with the retention and disposal schedule.

To Be a Model of Best Practice

Information Security – continuous improvement and development

Strategic Aim (6) – To ensure information security is appropriate, proportionate, measured, and part of business as usual.

Tactics:

- Assess and prioritise the control set contained within ISO27002 according to the level of risk and develop a programme for a phased implementation.
- Build ISO27002 controls into any new systems development.

Indicators of success

1. The confidentiality, integrity and availability of ICO information is maintained.
2. Continued compliance with the GSi code of connection which is based on the controls contained within ISO27002.
3. Compliance with the Government Security Policy Framework which is based on the controls contained within ISO27002.
4. Relevant controls are present in new systems.

To Be a Model of Best Practice

Compliance on the front foot

Strategic Aim (7) – To ensure compliance is always considered and built into initiatives at an early stage.

Tactics

- Provide input into IT development projects to ensure new or changed systems are capable of compliance.(ST-LT)
- Be alert to activities and events around ICO ensuring any compliance impacts are highlighted, understood and actioned.(ST-LT)
- Ensure internal compliance impacts are identified through the business planning process.(ST)
- Ensure internal compliance considerations are incorporated into the new corporate project management process.(ST-MT)
- Act as consultees for new ICO guidance providing feedback and another view about the practical considerations of what is being proposed.(ST-LT)
- Network with other information rights practitioners sharing best practice.(ST-LT)

Indicators of success

1. No extra costs – costs can be incurred if a compliance weakness is detected late and a remedy is needed.
2. Time is saved. It can take longer to deal with a compliance issue identified late than at the beginning of the process.
3. A test bed for new ICO guidance provides another view about the practical considerations of what is being proposed.

To Be a Model of Best Practice

Internal Compliance – Governance

Strategic Aim (8) – To ensure that robust governance arrangements are in place to monitor and steer the internal compliance programme of work.

Tactics

- Ensure that the governance arrangements for internal compliance are included as part of the corporate review of internal committees and boards.(ST)
- Ensure that internal compliance risks are identified and managed through ICO's corporate risk management process.(ST-LT)
- To increase the visibility of internal compliance matters at senior levels by providing a quarterly report to the Executive Team and the Audit Committee on internal compliance matters with ad hoc reporting on any significant internal compliance incidents or issues.(ST)
- To carry out regular reviews of the strategy to ensure its currency and effectiveness. (MT- _LT)

Indicators of success

1. The Executive Team, Management Board and Audit Committee are fully sighted about internal compliance matters.
2. Internal compliance risks are managed as part of a corporate risk management process and not in isolation.
3. Close monitoring of the programme of work will identify any deficiencies and ensure remedies are implemented.