Findings from the ICO's consensual FOI audits of the Northern Ireland Civil Service Departments

October 2020 to April 2021

Table of Contents

Introduction

The Information Commissioner is responsible for enforcing and promoting compliance with data protection legislation, as well as the Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations (EIR). Section 47 of the FOIA provides provision for the Commissioner to assess whether a public authority is following good practice, including compliance with the requirements of this Act and the provisions of the codes of practice under sections 45 and 46.

Approach

The ICO carried out a programme of audits to provide the Information Commissioner and the core departments of the Northern Ireland Civil Service (NICS) with an independent assurance of the extent to which the information handling practices conform with the codes of practice under sections 45 and 46 of the FOIA.

The nine NICS core departments participated in the consensual audits. Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with the Freedom of Information legislation.

This report highlights our findings. It is intended to help the departments recognise where they can make improvements in these areas. No individual departments are named in this report.

When conducting these audits, ICO auditors assessed the controls the departments had in place for Freedom of Information (FOI) and how effective those arrangements were. Where risks were identified, recommendations have been made to mitigate these and improve assurance against specific controls.

Determining compliance

To assist NICS departments in implementing the recommendations each has been assigned a priority rating (urgent, high, medium or low) based upon the risks that they are intended to address. The ratings are assigned based upon the ICO’s assessment of the risks involved.

For example, an urgent priority rating was attached to recommendations addressing clear and immediate risks to the data controller’s compliance with FOI and data protection legislation. High priority recommendations addressed risks which departments should tackle at the earliest opportunity.

The audit was broken down into 16 domains (See table 1 below). Each domain was given a rating based on how compliant the department was in that area and then a corresponding recommendation with priority rating was added, when required. We made 167 recommendations across the nine departments. 8% (14) of these were assessed as urgent and 43% (71) were assessed as high priority.

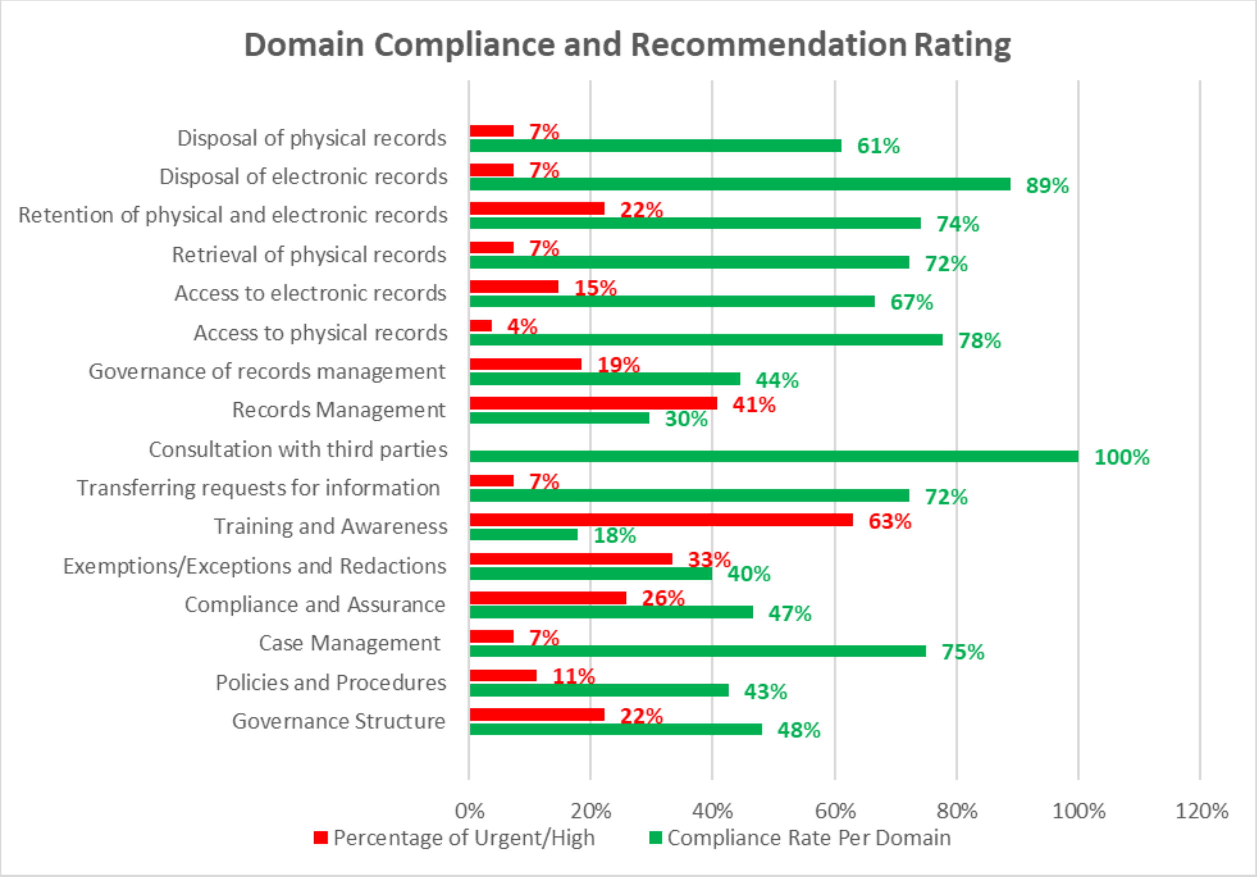

Table 1: Domain Compliance and Recommendation Rating

Audit domain compliance

As described in the "Determining compliance" section, a rating was used to rate a department's compliance against each of the control measures within the domains. The ratings were then collated to give an overall compliance rating for that domain. This section of the report provides details of the domain compliance ratings.

Governance structure

- Many departments have appointed an individual who sits at board level (usually a Senior Information Risk Owner, SIRO) and is assigned to be accountable and responsible for the department's FOI compliance.

- Reporting structures are in place providing ongoing oversight of the department's compliance with the legislation.

There were several areas, split over numerous departments, where recommendations have been made to help departments to improve their governance structure in relation to FOI.

- Key strategic roles within some departments had not been fully documented within the policies and procedures. Without formally documenting individual responsibilities, including at senior management level, compliance will not be prioritised and may result in noncompliance.

- It was found that all departments do not seek clarification that staff have read and understood relevant policies and procedures relating to FOI compliance. Without this confirmation the departments cannot ensure staff are working in compliance with their statutory obligations.

- No formal procedures are in place in any of the departments for the reallocation of staff to provide help in response to higher than usual volumes of requests for information. If there are insufficient resources, then individuals will be overworked. Responses may be delayed beyond statutory deadlines, or staff may make errors of judgement in determining what information to provide or withhold.

Policies and procedures

- ICO auditors found that all departments have documented policies and procedures which are detailed enough to provide staff with a basic guide through the FOI process. Staff can access these policies and procedures through their department's intranet site.

- ICO auditors also found that the majority of departments have developed a method for alerting staff when the relevant policies or procedures have been changed.

There were several areas, split over numerous departments, where recommendations have been made to help departments to improve their policies and procedures.

- There is limited document control information in support of the policies and procedures. Having effective document controls provide a clear audit trail for review and updates. This helps to ensure a consistent approach is applied across all policies, procedures and guidance.

- The process for disseminating policy changes does not allow for tracking or assurance that changes or updates to policies are read or understood by all staff. This means that in these cases there is no assurance that all staff will operate in line with the most up-to-date arrangements.

- ICO auditors found that the information some departments provide to the public does not state that the department may have to consult other public authorities or third parties to reach a decision on whether the requested information can be released. This means requesters may not be aware that third parties are being consulted regarding their request for information.

Case management

- ICO auditors found that in the majority of departments, where staff required further details in relation to a request, procedures are in place to help guide them in requesting clarifications with applicants in a timely manner and in compliance with FOI. During audit interviews, most staff were able to demonstrate an understanding that the aim of clarifying a request is to be able to distinguish all the information sought, not to determine the aims and motivations of the applicant.

- In instances where staff have communicated with requesters for clarification on the request, but the requester fails to provide it, the majority of departments have established procedures to ensure that any information relevant to the request which has been successfully identified should be disclosed, provided that an exemption does not apply.

- ICO auditors found that the majority of departments have procedures in place in relation to fee charges. In instances where applicants indicate that they are not prepared to pay a fee notification, the departments have processes in place to consider what information they could disclose free of charge.

There were several areas, split over numerous departments, where recommendations have been made to help departments to improve their case management controls.

- Requesters are not always being provided with details of their right to ask for an internal review (IR) and their subsequent right to complain to the ICO, when being contacted for additional information.

- The FOI procedures for staff provided as evidence for the audit by several departments did not provide staff with guidance on how to identify and handle vexatious requests for information.

- Although the majority of departments provide guidance to staff on how to seek clarification from a requester, some departments did not. This also includes guidance on fee charging and providing an indication of what, if any, information could be provided within the cost ceiling.

Compliance and assurance

- ICO auditors found that in the majority of departments there is a log kept of all requests. The logs were comprehensive and formed part of the reporting mechanisms that provide oversight of requests and help departments meet their statutory deadlines.

- There is a review of all compiled responses before they are provided to the requester, to ensure quality and validity.

- Where the outcome of a complaint is a decision that information should be disclosed which was previously withheld, the information in question is disclosed as soon as practicable and the applicant is informed how soon this will be.

There were several areas, split over numerous departments, where recommendations have been made to help departments to improve their compliance and assurance controls.

- ICO auditors found that the majority of departments' target times for dealing with complaints are not published and in some cases are not subject to regular review. Under Section 45 of the FOIA code of practice each public authority should publish its target times for determining complaints and information as to how successful it is meeting those targets.

- Some reviews are conducted by staff that would have been involved in collating the original response, leading to a potential conflict of interest in their ability to objectively review their own work.

- The Commercial Conditions for Supplies Contract and Services Contract and the Commercial Conditions of Contract for ICT do not refer to all the standard FOI and EIR clauses.

- Some departments have not formally identified where they are interdependent with other organisations for the handling of requests which means there is no assurance that all relevant information held by third parties will be requested and provided for such requests.

Exemptions/exceptions and redactions

- ICO auditors found that the majority of departments provide documented procedures for the application of exemptions or exceptions. Where a request is refused based on an exemption provision, the response from most departments to the applicant notified them of the complaints procedure (or stated that it does not have one). The responses also provided full details of the department’s own complaints procedure, including how to make a complaint and informed the applicant of the right to complain to the ICO under section 50 if still dissatisfied following the authority's review.

- There is also evidence within most departments of an oversight or approval process for the use of exemptions.

- The majority of departments have a documented process for the use of redactions agreed by senior management.

There were several areas, split over numerous departments, where recommendations have been made to help departments to implement improvements to their exemptions or exceptions and redactions controls.

- ICO auditors identified in most departments that staff responsible for the application of exemptions and redactions do not receive adequate training to carry out this task. Additionally, if challenges are made they are unable to respond with a full understanding of what is required.

- At least one department was found to provide very limited resources for staff to refer to for guidance on the use of exemptions in FOI request responses.

- Where there is no approvals process in place, cold-case dip sample checks are not carried out to check the quality of the redactions and exemptions ensuring all information has been correctly withheld. If the quality of redactions and exemptions are not monitored, there is a risk that staff may inadvertently release or withhold information incorrectly in response to a request.

Training and awareness

- ICO auditors found that the majority of departments provide staff with regular reminders of how to recognise FOI requests through newsletters or emails.

There were several areas, split over numerous departments, where recommendations have been made to help departments to improve their training controls.

- In some departments the success of the induction training is reliant on new starters reading and familiarising themselves with policies and procedures. There is no assurance that staff have read and understood the contents of the documentation. This means that staff could be unknowingly acting in breach of internal policy or FOI legislation.

- It was found that there is no formal requirement for refresher training to be completed within most departments. For those staff with limited FOI involvement, their understanding could diminish over time even though they still have documented responsibilities.

- It was identified with some departments that specialist training for staff in individual business areas with responsibility for handling FOI requests has been developed, however it is only delivered on request and not compulsory and current provisions cannot accommodate all relevant staff. This means that staff with direct involvement in handling requests may not have sufficient knowledge to carry out this role effectively or in line with organisational or statutory requirements.

- Some departments do not maintain records of the FOI training received by all staff. If the departments cannot demonstrate that they have provided training, they have no assurance that comprehensive training has been carried out. By not having oversight of training levels across the department senior management have no assurance that comprehensive training has been carried out.

- A minority of departments have access to eLearning applications. Some staff informed ICO auditors that they had heard about the training, but not completed it or had no knowledge of it.

Transferring requests for information

- All departments have put arrangements in place to determine which records should be selected for transfer to the Public Record Office of Northern Ireland (PRONI).

- The majority of departments have guidance for staff to ensure that third parties are aware of the public authority's duty to comply with the FOIA.

There were several areas, split over numerous departments, where recommendations have been made to implement improvements to their transferring requests for information controls.

- ICO auditors found that procedures, within a small percentage of departments, do not provide guidance where a request is transferred from one public authority to another to ensure the receiving authority complies with its obligations under Part I of the Act in the same way as it would in the case of a request that is received directly from an applicant.

- Within some departments the process for transferring records to archives is not outlined in procedures. If staff receive a request for information now held by PRONI and have no guidance in place in how to deal with these requests, then there is a risk that staff may take an inconsistent approach on how these requests are dealt with.

Records management organisation

- In the majority of departments, ICO auditors found that there are appropriate organisational arrangements in place to oversee the records management (RM) function.

- In the majority of departments, senior manager responsibility for the strategic direction and oversight of records management has been assigned to an executive board member.

- Most departments were able to demonstrate that there is an RM policy framework in place, that was subject to senior management approval and that periodic reviews were carried out to ensure it aligns with the latest guidelines.

There were several areas, split over numerous departments, where recommendations have been made to help departments to improve their records management controls.

- Responses provided during the ICO audit were inconsistent in their description of the provision for RM training and whilst it was evidenced that some training modules were in place there was no evidence to suggest that, apart from the Electronic Records Management System training, any of the additional training courses are compulsory or refreshed for all staff. This means that staff may not be aware of their responsibilities for RM and may operate outside of organisational requirements.

- During the audit some staff were unable to recall the last time they completed RM training. Without completing regular training on RM there is a risk staff maybe not be able to fulfil their responsibilities to handle data appropriately and keep records secure.

- It was reported in some departments that Information Asset Owners (IAOs) across each business area were responsible for ensuring that their business areas follow the Records Management Policy. However, there is no available job description for these roles. This means that the departments could not demonstrate that their IAOs have been formally assigned this responsibility.

- ICO auditors found that some departments do not provide any specialist training to IAOs to enable them to fulfil their responsibilities. In the majority of cases the role of IAO is allocated to the head of a branch rather than to experienced individuals which means that some IAOs do not have the relevant knowledge to fulfil the requirements of the role.

Governance of records management

- ❖ Although there were some weaknesses in this area, ICO auditors found that the majority of departments have a comprehensive inventory or asset register in place, which is regularly reviewed.

There were several areas, split over numerous departments, where recommendations have been made to help departments to improve their governance of RM controls.

- ➢ ICO auditors found that information audits had not been completed for five years and in some cases longer. As a result, those departments that have not conducted an information audit may not have a clear and accurate record of all the information held.

- ➢ Within the majority of departments ICO auditors found that IAOs do not provide regular evidence-based assurance that their asset registers have been reviewed and updated (where relevant) and that they are sufficiently managing their information assets. If information assets are not adequately identified and managed there is a risk that these departments may be in breach of information management legislation and may not be able to evidence effective governance and oversight of its information risks.

- ➢ ICO auditors identified that a departmental data flow map for personal data had not been carried out. Without having documentation demonstrating how personal data flows into, through, and out of the department, all the departments risk processing personal data without being organisationally aware of it and subsequently not applying proper controls to this processing activity.

Access to physical records

- ❖ ICO auditors found that the majority of departments maintained appropriate access controls which helped mitigate the risk of unauthorised access to physical records.

There were several areas, split over numerous departments, where recommendations have been made to help departments to improve their access to physical records controls.

- ➢ Although all departments have a RM policy in place, within a small number of departments there is limited information in the policy about the storage of physical records and the controls that are in place to ensure they are not accessed inappropriately.

- ➢ In a small number of departments there was limited evidence to show there was oversight of which staff have accessed physical records. Without having an audit trail in place that demonstrates who has accessed physical records the department cannot demonstrate compliance with Article 5.f. of the UK GDPR.

Access to electronic records

- ❖ The majority of departments audited provided evidence of policies and procedures documenting the arrangements for the access and security of electronic records. These were used to promote accepted standards and good practice. This helps ensure that the department's access control process is formalised and documented, and appropriate to the environment of the department.

- ❖ There was also evidence that records are maintained by Enterprise Shared Services (ESS) of the access permissions to electronic records granted to users.

There were several areas, split over numerous departments, where recommendations have been made to help departments to improve their access to electronic records controls.

- ➢ Whilst ESS create user accounts, the business areas are responsible for assigning user groups to document containers. It was reported to ICO auditors that some variation exists in the way that these controls are managed meaning that users may retain access to containers after they have moved to a different business area or is not always in line with requirements.

- In a small number of departments, no evidence was presented to show that access control procedures are documented so staff who manage them may not always be aware of their responsibilities.

- ICO auditors also determined from the evidence provided there is no formalised approach to the periodic review of access controls. This is important because there is a risk of inappropriate access to information if access controls are not subject to periodic review.

Retrieval of physical records

- To ensure that personal information is not lost or misplaced the majority of departments have processes in place that allows them to always know the whereabouts of records and the movement of records and provide an audit trail of all record transactions.

- ICO auditors found that manual records are transferred in accordance with the security classification and this classification must be maintained at the receiving end.

There were several areas, split over numerous departments, where recommendations have been made to help departments to improve their retrieval of physical records controls.

- Some departments do not regularly review their policies, and the policies that are in place are not detailed enough to provide guidance to alternative distribution methods when post and fax are not options.

Retention of physical and electronic records

- ICO auditors found many departments have produced a retention schedule based on business need with reference to statutory requirements. The schedules demonstrate sufficient information is being captured for records to be identified and disposal decisions put into effect.

- For some departments, the retention schedule is regularly reviewed to make sure it continues to meet business and statutory requirements.

There were several areas, split over numerous departments, where recommendations have been made to help departments to improve their retention of physical and electronic records controls.

- ➢ In a small percentage of departments, ICO auditors found that documentation was not being updated in line with the document review schedule.

- ➢ One department does not carry out compliance checks to ensure that IAOs are disposing of physical records in line with the Retention and Disposal Schedule as the destruction of records are currently on hold at the department until the Draft Retention Schedule can be reviewed by PRONI and authorised by the NI Assembly.

Disposal of electronic records

- ❖ The majority of departments currently dispose of their electronic records in line with the Retention Schedule.

- ➢ It was found that one department is prevented from carrying out deletions in line with the current retention schedule until it has received approval from PRONI and the NI Assembly. This means they are currently holding information that has exceeded its planned retention period.

Disposal of physical records

- ❖ There is evidence in the majority of departments that all paper-based records containing personal data are destroyed in line with the Retention Schedule.

- ❖ There is evidence of management sign off or approval prior to the disposal of physical records and methods of destruction used for physical records are appropriate to prevent disclosure of personal data prior to, during and after disposal.

There were several areas, split over numerous departments, where recommendations have been made to help departments to improve their disposal of physical records controls.

- ➢ Lack of evidence was provided in some cases that failure to destroy physical records in line with the retention schedule is reported as an incident.

- It was reported during audit interviews that a contract dispute with the current on-site disposal contractor in one department has meant that not all physical records have been destroyed in line with the retention schedule recently. Whilst some records are being manually shredded by staff this is not suitable for large volumes of physical records due for destruction. There is also an issue with getting shredded waste collected and destroyed appropriately because of the dispute. If methods of destruction are not appropriate, then the department will find that it has breached Article 5 (1) (f) and 32 of the UK GDPR.

- In one case a large volume of legacy records has not been fully identified and in another some records have not been fully indexed. Therefore, until these records are fully identified and indexed there remains the risk of over-retention of records.

Resources

The ICO website has resources available to aid public authorities and the public's understanding of the FOIA.