Information Commissioner's Office

Internal Audit Report: Information Governance

January 2021

mazars

Contents

mazars

01 Introduction

As part of the agreed Internal Audit Plan for 2020/21 we have undertaken a review of the Information Commissioner's Office (ICO) arrangements for information governance. We have reviewed key elements of the ICO's arrangements to ascertain whether processes and controls are designed and operating effectively.

The audit assessed risks in the following areas:

- Policy and procedures;
- Roles and responsibilities;
- Information requests;
- Data processing;
- Information communication;
- Staff training; and
- Management information and reporting.

Full details of the risks covered are included in **Appendix A1**

We are grateful to the Director Risk and Governance, Head of Risk & Governance, Head of Internal Services, Group Manager Information Management, Group Manager Risk and Governance Department, Information Security Manager and other staff for their assistance during the audit.

This report summarises the results of the internal audit work and, therefore, does not include all matters that came to our attention during the audit. Any such matters have been discussed with the relevant staff.

The fieldwork for this audit was completed whilst government measures were in place in response to the Covid-19. The fieldwork for this audit has been completed and the agreed scope fully covered. Whilst we had to complete this audit remotely, we have been able to obtain all relevant documentation and/or review evidence via screen sharing functionality to enable us to complete the work.

02 Background

Organisations are expected to control ever-increasing data volumes as developments in information technology allow data to be efficiently collected, stored and analysed. This elevates the risks within information management as the scope for mismanagement increases with the volume of data.

Modern responses to information risk management include the incorporation of information governance. Good information governance practices take into account several considerations including: storage, communication & transference of information, compliance with laws, training and performance reporting.

Storage, communication and transference of information should be supported by a reliable IT infrastructure with developed cybersecurity enhancements. Although ultimately solutions for information storage and communication is highly dependent on organisational needs, nonetheless whether cloud or physical servers are used these should be robust in order to avoid cybersecurity breaches. The storage of both carbon copy and electronic information requires retention schedules to be considered, often this in the form of a centralised list of data assets identifying how long the data asset is kept and when they are expected to be destroyed.

The Data Protection Act 2018 is the UK's implementation of General Data Protection Regulations GDPR, an EU regulation. Retention schedules are one of the requirements under UK GDPR as personal data is often contained within information held by the organisation.

Under UK GDPR organisations are required to provide data subjects access to their personal data when a Subject Access Requests is made. This must be fulfilled within one calendar month of the request. Subject Access Requests (SARs) can be resource intensive where multiple SARs are received. Furthermore, ICO's status as a non-departmental public body requires the compliance of the Freedom of Information Act 2000 and as such applicable official information must be made available to requestors within 20 working days.

Freedom of Information (FOIs) requests and SARs require active management and tracking to ensure statutory timelines are met. This is

often overseen by a Data Protection Officer, a role that is required by public bodies under UK GDPR.

The responsibilities of the Data Protection Officer is officially set out within GDPR Article 39 and their remit will often include designing and leading on information training and performance reporting. At ICO the Data protection Officer role is held by the Director of Risk and Governance. In addition, the position of Senior Information Risk Owner is held by the Deputy Chief Executive Officer who has overall responsibility of information risk policy at ICO.

Towards the end of March 2020, the UK Government requested all "non-essential" workers to work from home as the UK entered into lockdown in response to Covid-19. Although Covid-19 has impacted many organisation including ICO, nonetheless information management and governance is continually practiced within ICO albeit delays were experienced for dealing with postal information requests.

03 Key findings

Assurance on effectiveness of internal controls

Substantial Assurance

Rationale

For the internal audit work carried out (please see Appendix A1 for the detailed scope and definitions of the assurance ratings), we have provided Substantial Assurance.

Overall, we have identified a number of well-established controls around information governance.

The audit has identified a number of weaknesses that should be addressed to further improve the control environment. For instance, our review identified issues which the ICO should address in the following areas: FOIs and SARs response times, completion of information asset registers, performance reporting, automation of the incident and breaches register and detail captured within the Information Management Standard.

Please see **Section 04** for further detail in respect of the recommendations made from our review.

3.1 Examples of areas where controls are operating reliably

- There are a range of policies related to information governance, including separate policies related to information security, retention and disposal schedule, information classification and a guidance for outlining the framework for information governance at ICO; this is captured within the Information Management Standard. These policies should help staff to understand good practices of information governance.

- The ICO has defined input required from different teams and staff members for the management of information governance. The SIRO chairs the Risk Governance Board and is the management lead for information governance. The DPO is responsible for providing guidance on operational information governance practices. Other teams involved include the Information Management, Information Access and Information Security teams which are involved in managing data assets, responding to information requests and providing security to information assets respectively.
- Good information governance requires a collective contribution within an organisation. The ICO encourages input from across the organisation through the allocation of roles including Information Asset Owners who are responsible for the data processed within their teams. Information Asset Managers act as deputies to the Information Asset Owners and is operationally responsible for the upkeep of information assets. Local Information Management Officers are staff members serving as points of contacts for best practice guidance for information management.
- The Information access team are responsible for responding to information requests including FOIs and SARs. There is an information request procedure for all staff which identifies information requests can come in multiple forms and may not directly be received by the information access team in the first instance. This helps staff identify what an information request may actually look like and the associated timescales involved with the different requests.
- ICO's position as a regulator is likely to attract greater scrutiny for its work. The ICO has a separate procedure document for information requests which are classified as "potentially high profile". Such requests are identified as issues covered within the media where ICO may have involvement, high profile investigations, requests made by journalists and any requests for ICO handling of internal compliance with GDPR. The process requires notification of such requests to the Press team, the SIRO and DPO.
- ICO is able to understand the information assets it holds through the Records of Processing Activities (ROPA). It tracks the categories of data, purpose of processing, and security measures in place and retention schedules. A ROPA is a requirement according to Article 30 of GDPR and as such the ICO is able to demonstrate adherence to Article 30, however we have raised a recommendation to develop separate information asset registers which would provide greater detail on the information assets held.
- The avenues of internal information communication and how information may be stored electronically and physically is identified within the Information Management Guides. Digital storage may include SharePoint EDRM, Casework Management system depending on the information asset. Temporary storage and work requiring collaboration is identified as permissible to be stores within Microsoft Teams.
- External communications to and from the ICO, such as contractors typically utilises secure sharing portals where this can be facilitated. Procurement will ask the Information Security team to evaluate the suggested systems used to share information. Where there is no secure information sharing facility available, information would be sent by email. We understand emails are encrypted, however, this did not form part of our testing.
- A communication plan is in place which sets out the year ahead for communications to the wider organisation including best practices on SharePoint, training reminders and any information management related communications. This helps the ICO to organise their regular engagement with staff to remind them of the importance of information governance and circulate best practices.
- There are a suite of information management training including information governance training as part of induction, workshop based delivery of data protection, GDPR and FOR and also e-learning.
- Information governance and security matters including incidents and breaches are disseminated though the quarterly Information Management Community and the monthly Risk Governance Board.

3.2 Risk management

There are no direct information management risks as identified within ICO's Risk and Opportunity Register from November 2020. This is not uncommon across the sector since information management is typically a business as usual operation and would unlikely feature within a strategic risk register unless there has been an increase in information breaches or cybersecurity incidents.

There is however a wider risk encompassing compliance culture which has a gross risk score of Red 20: *R73* ***Compliance culture:*** *(Cause) Risk that as demand and capacity increase and/or changes the ICO's infrastructure and accountability culture is unable to (Threat) keep up with the pace of change to comply with legal and other obligations expected of a modern regulator (Impact) impacting upon its ability to maintain and increase public trust and bean effective and knowledgeable regulator.*

The ICO has identified the information governance policies and security manual as the sources of mitigating controls. An action for ongoing training of information rights compliance and its oversight by the Risk and Governance Board also aid to mitigate the risk.

We confirmed as part of the audit, information governance and information security policies are in place, in addition to ongoing training and monitoring by the Risk and Governance Board.

3.3 Value for money

Value for money within information governance is ensuring robust controls are in place to facilitate smooth communication, prevention of data breaches, ensuring information rights are respected and compliance is met with data laws.

ICO is able to demonstrate value for money through the dedicated channels of communication including an organisation wide file architecture; SharePoint EDRM and Microsoft Teams for collaborative working. The accessibility of electronic file storage and a video conferencing platform standardises how information is shared both internally and externally thereby avoiding staff uses of unsecure communication tools.

Preventative controls currently adopted by other organisations include additional email recipient confirmation for email users to complete before the release of email to be sent. This allows for email users to re-evaluate recipients are indeed the intended recipients thereby reducing breaches of information to third parties. Although this is control is currently not in place at the ICO, this could be considered as we noted the information incidents and breaches register mainly contains incidents relating to disclosure breaches.

The ICO has good controls adopted including process flowcharts, information requests procedures and late referral tracking for information requests referrals made to the Information Access team. These controls aim to facilitate the Information Access Team to deliver information responses in line with statutory timelines, however we noted two FOIs and one SAR were not responded to within the statutory timelines to which we documented our observation within section 4 of this report.

3.4 Sector comparison

ICO's Information Governance framework and its information management practices are considered to have good controls although work is still required around Information Asset Registers which is discussed within our recommendations under Section 4 of this report.

The ICO is required to maintain a Records of Processing Activities (ROPA) under GDPR Article 30. Although the ICO has fulfilled this requirement we note other organisations with this requirement will typically utilise both a ROPA for high level overview and Information Asset Registers for a closer review of the type for data held.

In organisations with a developing or initial information governance framework, SIROs are not typically in place as the role is not defined within law. As such, there is clear lack of responsibility and accountability for ownership of information management especially where the DPO is not undertaken by a senior member of management. At ICO the SIRO is currently held by the Director of People and Infrastructure.

04 Areas for further improvement and action plan

Definitions for the levels of assurance and recommendations used within our reports are included in Appendix A1.

We identified areas where there is scope for improvement in the control environment. The matters arising have been discussed with management, to whom we have made recommendations. The recommendations are detailed in the management action plan below.

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
4.1	**Information requests and subject access requests** *Observation:* Freedom of information (FOI) and subject access requests (SAR) are required to be responded to within 20 working days and one calendar month respectively as outlined within legislation. We tested a sample of 10 FOIs and found two requests were not responded to within 20 workings days (response times of 22 days and 25 days). We also tested a sample of 10 SARs and noted one that was responded to outside the timeline of one calendar month. The request was fulfilled within 44 days. For each of the FOIs and SAR outside the timeframe there was no documentation to support an extension of time. Additionally, there was one SAR sample which was sent as a request via post on the 21/07/2020. The request was not responded to until 03/12/2020 due to office inaccessibility from Covid-19. We understand arrangements have since been made to open and scan post held within the offices. As such the SAR request by post was uploaded to ICO's	The ICO should: 1. Ensure FOIs and SARs are responded to within the timelines outlined within legislation. Where there are circumstances which extend the length of time required to respond to request, these should be well documented for a clear audit trail. 2. Update its website informing the current status of accessibility of information requests made by post, and where a delay is still expected this should be communicated fully and alternative arrangements should be made aware to website visitors. 3. Send confirmation responses to information requests should be adopted for all information requests.	2	1. Agreed all of our processes aim to respond to FOIs and SARs within timelines. We do already document reasons for extensions. We are actively looking at resourcing for the team and process efficiencies. 2. The website comms are under review so this is to be decided but good progress has been made on the post backlog. 3. This has been assigned to a specific post to ensure there are no gaps and is now fully implemented.	April 2021 Elizabeth Baxter Decision on update by end of April 2021 / Joanne Butler Complete / Elizabeth Baxter

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
	case management system on the 10/11/2020 and the response date of 03/12//2020 effectively places the response within 23 days. The lengthy time elapsed for the SAR requested via post could have been negated through communication on ICO's website on the closure of offices and the unavailability of post accessibility. We noticed the ICO did not update the website notifying website visitors of the office closures and limited accessibility to post during lockdown. Furthermore, we noted acknowledgements of receipt of FOIs and SARs are not consistently sent to requestors for confirmation of request. *Risk:* The ICO is unable to respond to FOIs and SARs in accordance with legislation.				
4.2	**Information asset registers** *Observation:* ICO's website has guidance advising that Information Asset registers are a tool for recording "*assets, systems and applications used for processing or storing personal data across the organisation*". The ICO currently does not have individual information asset registers for all the different information assets held by different teams within the ICO. Instead it has high level registers in the form of the Corporate Information and Information Management registers. Although the ICO currently does not have individual information asset registers in place for all teams, it does have a Records of Processing Activities	The ICO should implement an information asset register for all teams and information assets in place. A semi-annual assurance statement should be made by the DPO to the SIRO on the contents of the ROPA and its accuracy.	3	Agreed, we will implement this for all teams. We will develop an assurance statement. Timescales to be confirmed.	End September 2021 / Alan McGann December 2021 / Alan McGann

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
	(ROPA) which acts as a high level record of information assets and the reason for holding such information. As such the ICO is aware of the information it holds, however, individual information asset registers allow a greater understanding and breakdown of the information assets held. We understand the ROPA is a live document and we were unable to compare any previous iterations of the ROPA to document change in information assets. *Risk:* The ICO does not understand the data and information it holds.				
4.3	**Performance reporting** *Observation:* The number of FOIs and SARs requests and completions are currently not discussed within any of the avenues of management reporting including the Information Management Community or the Risk Governance Board. Furthermore, there are no key performance indicators set for information governance at the ICO. *Risk:* Lack of monitoring and reporting results in no action to address issues.	The ICO should consider reporting the number of FOI and SAR requests and their completions to the Risk Governance Board so resourcing requirements can be identified in advance. A suite of information management and governance key performance indicators should be set and delivery against the KPIS should also be reported to the Risk Governance Board.	3	Performance of the IA Team is discussed across management (including Management Board) The RGB was a new Board but the Information Governance Group will be reporting on FOI and SAR performance to the RGB on a regular basis. Although we do have a number of KPIs set for information governance we are developing reporting through the IGG to RGB.	June 2021 / Joanne Butler June 2021 / Joanne Butler

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
4.4	**Automation of incident forms** *Observation:* The incident security log is used to record information security breaches and near misses. The Log is maintained by the Information Security team, and incidents reported to the team are updated by the Information Security Manager. There is an opportunity for the automation of the incident security log for staff to directly complete a web form and its contents to directly populate the register in order to avoid transposition errors. *Risk:* Information incidents and breaches are not recorded accurately.	The ICO should consider automating the incident capturing within the incident security log.	3	We have considered automation but this is not currently on our roadmap for delivery. There is no evidence that information incidents and breaches are not recorded accurately.	Completed / Alan McGann
4.5	**Policy and procedures** *Observation:* ICO's Information Management Standard is a document outlining in brief, ICO's framework for information governance. Within the standard it highlights several key roles with reference to the Information Risk Management Framework where roles and responsibilities are captured in greater detail. We noted the Information Risk Management Framework currently does not include the role of the DPO and its associated responsibilities. The Information Management Standard also provides very little information relating to training delivery, the other teams involved in information management including the Information Access,	The ICO should update the following for its guidance documents; 1. The role of the DPO within the Information Risk Management Framework. 2. The involvement and responsibilities of the Information Access, Information Management and Information Security teams within the Information Risk Management Framework and Information Management Standard. 3. Information related training, analysis and evaluation within the Information Management Standard.	3	We will review our documents bearing in mind the detail of these recommendations and update where needed.	30 June 2021/Helen Ward/Alan McGann

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
	Information Management, and Information Security teams. Additionally, the governance flow of performance monitoring such as reporting to the Information Management Community and the Risk Governance Board is not outlined within the Information Management Standard. *Risk:* Management and accountability of information governance is not made clear within the ICO, resulting in information governance failures.	4. Performance reporting and frequency to the relevant boards and committees within the Information Management Standard.			

A1 Audit information

Audit Control Schedule	
Client contacts:	Louise Byers, Director Risk and Governance (Data Protection Officer) Joanne Butler, Head of Risk & Governance Helen Ward, Head of Internal Services Iman Elmehdawy, Group Manager- Information Management Elizabeth Baxter, Group Manager, Risk and Governance Department Danny Langley, Information Access Manager Jessica Lalor, Senior Information Access Officer Steven Rook, Information Security Manager
Internal Audit Team:	Peter Cudlip, Partner Darren Jones, Manager Cooper Li, Internal Auditor
Finish on site / Exit meeting:	04/01/2021
Last information received:	27/01/2021
Draft report issued:	2/02/2021
Management responses received:	24/02/2021
Final report issued:	03/03/2021

Scope and Objectives

Our audit considered the following risks relating to the area under review:

- **Policy and procedures:**
  No robust information handling policies, or staff are unaware of how to comply with policies and develop inconsistent approaches.
- **Roles and responsibilities**
  Lack of accountability for information management arrangements which leads to poor or no management of information security and data protection risks.
- **Information requests**
  Inadequate process to handle freedom of information or subject access requests
- **Data processing**
  The ICO does not understand the data/information it holds. This includes:
  - What records are held and by which service/department
  - Who has access to the records
  - Where the records are stored and whether this is appropriately restricted/secured, where required
  - What records are shared with other parties and whether this contains sensitive and/or personal data; and
  - When records should be destroyed /deleted in line with internal policy and regulations
- **Information communication**

The ICO does not use appropriate methods to communicate information and data, particularly where this is sensitive and/or personal data.

- **Staff training**
  Mishandling of information is increased through lack of information security and data protection training.
- **Management information and reporting**
  Lack of monitoring and reporting arrangements resulting no action to address issues or near misses identified or poor decision making.

The objectives of our audit were to review the adequacy and effectiveness of controls and processes for information governance with a view to providing an opinion on the extent to which risks in this area are managed. In giving this assessment, it should be noted that assurance cannot be absolute. The most an Internal Audit service can provide is reasonable assurance that there are no major weaknesses in the framework of internal control.

The limitations to this audit was that testing was conducted on a sample basis. This is not a substantive audit of the financial records of the organisation.)

Definitions of Assurance Levels	
Level	**Description**
Substantial Assurance:	Our audit finds no significant weaknesses and we feel that overall risks are being effectively managed. The issues raised tend to be minor issues or areas for improvement within an adequate control framework.
Adequate Assurance:	There is generally a sound control framework in place, but there are significant issues of compliance or efficiency or some specific gaps in the control framework which need to be addressed. Adequate assurance indicates that despite this, there is no indication that risks are crystallising at present.
Limited Assurance:	Weaknesses in the system and/or application of controls are such that the system objectives are put at risk. Significant improvements are required to the control environment.

Definitions of Recommendations	
Priority	**Description**
Priority 1 (Fundamental)	Recommendations represent fundamental control weaknesses, which expose the organisation to a high degree of unnecessary risk.
Priority 2 (Significant)	Recommendations represent significant control weaknesses which expose the organisation to a moderate degree of unnecessary risk.
Priority 3 (Housekeeping)	Recommendations show areas where we have highlighted opportunities to implement a good or better practice, to improve efficiency or further reduce exposure to risk.

Statement of responsibility

We take responsibility to Information Commissioner's Office ICO for this report which is prepared on the basis of the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

This report is confidential and must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation amendment and/or modification by any third party is entirely at their own risk.

Contacts

Peter Cudlip
Partner, Mazars
peter.cudlip@mazars.co.uk

Darren Jones
Manager, Mazars
darren.jones@mazars.co.uk

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services*. Operating in over 90 countries and territories around the world, we draw on the expertise of 40,400 professionals – 24,400 in Mazars' integrated partnership and 16,000 via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

*where permitted under applicable country laws.

www.mazars.co.uk