Information Commissioner's Office

Internal Audit Report: Guidance development

March 2023

FINAL REPORT

Contents

01 Introduction 1

02 Background 1

03 Key Findings 2

3.1 Examples of areas where controls are operating reliably 2

3.2 Risk Management 4

04 Areas for Further Improvement and Action Plan 5

A1 Audit Information 6

Contacts 8

Disclaimer

This report ("Report") was prepared by Mazars LLP at the request of the Information Commissioners Office (ICO) and terms for the preparation and scope of the Report have been agreed with them. The matters raised in this Report are only those which came to our attention during our internal audit work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, Internal Audit have only been able to base findings on the information and documentation provided and consequently no complete guarantee can be given that this Report is necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

The Report was prepared solely for the use and benefit the ICO and 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. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification by any third party is entirely at their own risk. Please refer to the Statement of Responsibility in Appendix A1of this report for further information about responsibilities, limitations and confidentiality.

mazars

01 Introduction

As part of the agreed Internal Audit Plan for 2022/23, we have undertaken a review of the Information Commissioner's Office's (ICO) key controls in relation to guidance development. Full details of the risks covered are included in **Appendix A1**.

The guidance the ICO produces includes, but is not limited to:

- Guidance for organisations on compliance with the laws they regulate;
- Guidance for the public on their information rights; and
- Guidance on how the public, and organisations, can access their services, make complaints, raise issues and find out more about the ICO's work.

Internal audit last reviewed the area of guidance development in 2018/19, with an 'Adequate' assurance rating given. As agreed with management, this audit in 2022/23 focused on guidance developed specifically for organisations on the laws the ICO regulates.

We are grateful to the Head of Assurance, Group Manager- Policy 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.

02 Background

As a whole-economy regulator, the ICO creates guidance for a wide range of different audiences. Guidance is produced for a variety of purposes across the eleven laws that ICO is the regulator for. The ICO has a statutory responsibility under the Regulator's Code to provide guidance to the organisations it regulates.

The ICO's new strategy, ICO25, was published and became live in November 2022, replacing the previous Information Rights Strategic Plan (IRSP). The strategy sets out the ICO's purpose as a regulator, which is 'empowering you through information'. A key activity to achieve this is through publishing guidance in line with strategy.

A Regulatory Policy Methodology Framework is in place which details seven steps to good policy making:

1. Identifying the issue;
2. Research and analysis;
3. Develop policy options;
4. Consultation (formal and informal);
5. Recommendation and decision;
6. Implementation;
7. Evaluation.

Since the previous review in 2018/19, the ICO has implemented a documented Guidance Governance Process which includes a Guidance Governance Group (GGG) to oversee the development of guidance. The GGG meet bi-monthly to review all proposed guidance and are responsible for ensuring that each is in line with the ICO's brand and objectives. Proposed projects also need to meet an identified need, be planned consistently, and have sufficient oversight relative to risk.

A lot of guidance at the ICO is developed by the Regulatory Policy team. This team is responsible for most core guidance for organisations in respect of Data Protection legislation, with other teams responsible for other regulations or other topics, or use-case specific guidance. Guidance is reviewed throughout the development process by relevant staff members and is also reviewed by the in-house Policy Legal Team if deemed necessary by the GGG.

Consultations are held with the expected audience in the form of public consultations or with bodies such as civil society organisations and industry designers if required.

Before publishing on the ICO website, guidance products are shared with the ICO's Communications Team. Dependent on the product, guidance may be subject to a full Communications plan, or an 'editorial review' which includes checking the document is in plain English. The Communications Team shares new guidance with external stakeholders in a variety of methods, including via posts on the ICO website and social media.

03 Key Findings

Assurance on effectiveness of internal controls
 **Substantial Assurance**

Rationale
The internal audit work carried out has provided **Substantial Assurance**. Please see Appendix A1 for the detailed scope and definitions of the assurance ratings. The ICO had already identified a number of improvements to the control environment for guidance development and were in the process of implementing them at the time of the audit. We have therefore not raised recommendations in relation to these matters. One 'Low' priority recommendation has been raised. Please see Section 04 for further detail in respect of the recommendation made and improvements to the controls current in progress.

Number of recommendations			
High	Medium	Low	**Total**
-	**-**	**1**	**1**

3.1 Examples of areas where controls are operating reliably

- To help to ensure consistency across guidance development, the ICO implemented a Guidance Governance Process in 2021. This is available on the intranet (IRIS) and sets out the responsibilities of the Guidance Governance Group (GGG), the project team, Corporate Communications and Economic Analysis. It also details project documentation requirements and the guidance sign off process.
- The ICO also has a Regulatory Policy Methodology Framework, last reviewed in May 2021, which explains how the ICO gathers information to inform decisions about whether guidance is the best solution to a particular policy issue, and if it is, what should be included in the guidance.
- We selected a sample of five job descriptions from 24 roles provided who are involved in guidance development. We confirmed that each of the job descriptions highlighted the need for the position to develop or contribute to policy/guidance.
- Staff developing guidance have access to the 'How-to Guide' which includes a link to the Regulators Code and states a requirement for all staff to have read this before planning a project.
- A Guidance Governance Group (GGG) is in place to review all proposed guidance and ensure that each project is in line with the ICO's brand and objectives. The Terms of Reference, last reviewed in March 2022, sets out the Group's objectives and responsibilities to supervise a clear and comprehensive guidance governance process.
- Proposals for new public guidance to organisations require a documented Guidance Plan for discussion at the Guidance Governance Group (GGG). The template includes the question: '*How do you plan to align your guidance with the ICO25 objectives?* We selected a sample of nine guidance products which have been published on the website since September 2022 and confirmed each of these products had been produced in line with the Guidance Governance Process, with a Guidance Plan submitted to the GGG

and approved before publication. The Guidance Plans had a link to either ICO25 or the previous strategy if before November 2022.

- We reviewed the GGG's bi-monthly meetings since March 2022 and confirmed each meeting had a standard agenda in place, documented minutes and new Guidance Plans were presented. Each meeting received updates on ongoing guidance products in the form of highlight reports.
- Prior to each bi-monthly GGG meeting, a meeting is held with the GGG and the Policy Legal team to ensure sufficient scrutiny has been given to all proposed guidance products. We have seen screenshots of calendars to confirm these were diarised before each bi-monthly meeting from March 2022 to March 2023.
- Between January and May 2022, the ICO ran a survey and events (a Listening Exercise) to hear directly from organisations, business and the public on what guidance is needed. As a result, a 'pipeline' project was developed. This aims to provide additional regulatory certainty by detailing what guidance the ICO has planned, what is currently being worked on and when products are due to be published.
- As an addition to the Regulatory Policy Methodology, staff have access to a range of information that can help them further determine whether guidance is needed on a particular issue including:
    - Media monitoring systems;
    - Journal subscriptions;
    - Input from Knowledge Services team;
    - Annual Strategic Assessment results, developed by Intelligence Team; and
    - Trend analysis on queries received via the helpline.

  For example, the November 2021 Strategic Assessment, completed by the ICO's intelligence team, identified an increased use of biometrics and AI in the workplace. This assessment, along with monitoring of media articles and analysis of complaints, helped to identify a need for guidance on this area and the Monitoring at Work guidance was developed as a result.
- There are five guidance levels and priorities which developers are required to assess their product against. The ratings are determined by risk and impact and have a corresponding approval process. For example, 'Level E+' requires Commissioner approval. For a sample of nine guidance products, we confirmed that each had the required sign off in line with its guidance level. New guidance products above Level 2 must be reviewed by the Policy Legal team. We confirmed for our sample of nine guidance products that legal input had been sought in line with requirements.
- The ICO has a Consultation Policy which applies to guidance production and outlines how the ICO will run formal consultations with external stakeholders and members of the public, including staff where appropriate. Guidance Plans have a section on proposed consultation which is reviewed by the GGG. For our sample of nine guidance products, we confirmed that these were subject to internal and/or external consultation, in line with the approved Guidance Plan. Some products were not yet sufficiently progressed to have required a consultation at their current stage.
- Corporate Communications allocate an Account Manager to each piece of guidance, and regular updates are given whilst writing draft guidance. Depending on the size and type of guidance, the project team and Corporate Communications will develop a Communications Delivery Plan.
- Guidance is promoted internally using the Iris staff intranet. Guidance published on the external website is shared internally via a 'Publishing Alert' email distribution list. There are also 'Know about' sessions, manager and team briefings and internal training. External promotion takes place using methods such as the annual Data Protection Practitioners' Conference, website publication, social media, press releases and the ICO newsletter.
- The ICO measures impact of guidance in a variety of ways including published impact assessments, user acceptance testing of website, market research, and media evaluation. We reviewed improvements the ICO has implemented to the guidance development process as a result of feedback. These include the implementation of version control on published guidance and ensuring future guidance is published with a 'must, should, could' view.

3.2 Risk Management

A review of the ICO's Corporate Risk and Opportunity Register (January 2023) highlighted there is no specific risk related to guidance development. The directorate risk register for Regulatory Assurance includes the following risk:

'Increasing expectations from government and other stakeholders for research led and evidenced based guidance, with economic analysis and formal consultation, while being concise and audience targeted, leads to inability to manage stakeholder expectations for regulatory guidance; damaging the ICO's reputation and relevance as a regulator'.

Risk is mitigated in this area through the Guidance Governance Process and oversight by the GGG. This oversight aims to ensure that each proposed guidance project is in line with the ICO's brand and objectives, meet an identified need and is planned consistently. A risk-based approach is taken to approval of guidance prior to issue.

The last internal audit in 2018/19 noted improvements to the guidance development process, namely a formal governance process to oversee the development of guidance for organisations. This has been implemented in the form of the GGG, with clear structures and guidance documentation in place. There are further areas of improvement that the ICO is working on in relation to implementing prioritisation, impact and evaluation frameworks to further strengthen the guidance development process.

04 Areas for Further Improvement and Action Plan

The ICO had already identified a number of improvements to the control environment for guidance development and were in the process of implementing them at the time of the audit. We have therefore not raised recommendations in relation to these matters. These relate to:

- Ensuring guidance is published with GGG approval – The ICO identified 'Top tips for games designers – how to comply with the Children's code' was published on 16 February 2023 on the ICO website without following the required GGG process. An internal review of the publication of this guidance is ongoing. The ICO is implementing an additional check by the Communications Team to confirm approval has been received prior to publication.
- Collating and taking forward lessons learnt - Whilst learnings are documented within the project Closedown Report, they are not collated and taken forward in a formal way. The ICO is looking to implement a process to use this data to inform process improvements.
- Developing a prioritisation framework - The Executive Team have highlighted that staff are prioritising activity including guidance in different ways, leading to inconsistent practices across teams. As a result, the ICO are in the process of developing a prioritisation framework.
- Measuring the impact and use of published guidance - The Economic Analysis directorate was set up in 2022 to deliver the ICO's obligations under the Regulators Code to provide impact assessments for guidance. They are in the process of developing a consistent method for collating and measuring the use and impact of published guidance. An Impact Assessment Framework is out for consultation and is due to be finalised and publicised in Summer 2023. The team is in the process of developing an Evaluation Framework to help the ICO provide a consistent and proportionate approach.

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

We identified an area where there is scope for improvement in the control environment. The matter arising has been discussed with management, to whom we have made a recommendation. The recommendation is detailed in the management action plan below.

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
4.1	**Consultation Policy** The Consultation Policy was last updated in December 2021. We were advised by the Corporate Governance team that this Policy is currently undergoing review, however there was no set review schedule in place. *Risk: Policies are out of date and do not reflect current practice. Staff are unaware of the correct processes to follow.*	The ICO should determine a review frequency for the Consultation Policy and update this in line with the schedule.	**Low**	Recommendation accepted. We will complete a review of the Consultation Policy and publish a new version by 31 December 2023. Following that we will review the Policy every 2 years.	31 December 2023. Adrian Price, Head of Regulatory Strategy

A1 Audit Information

Audit Control Schedule	
Client contacts:	Chris Taylor, Head of Assurance Elanor McCombe, Group Manager- Policy
Internal Audit Team:	Peter Cudlip, Partner Hannah Parker, Associate Director Jessica Holt, Assistant Manager
Finish on site/ Exit meeting:	10 March 2023
Last information received:	14 March 2023
Draft report issued:	28 March 2023
Management responses received:	30 March 2023
Final report issued:	30 March 2023

Scope and Objectives

Audit objective: To provide assurance over the design and effectiveness of the key controls operating in relation to the ICO's approach to guidance development.

- **Strategy -** Published guidance is not in line with the ICO 25 Strategy or wider broad obligations under the Regulator's Code.
- **Role and responsibilities -** Staff are unaware of their roles and responsibilities for guidance development.
- **Identifying needs and prioritisation -** Specific guidance needs are not identified due to lack of staff awareness, management information or poor stakeholder engagement. Guidance is not prioritised appropriately.
- **Guidance development -** Guidance production is not performed in line with agreed guidance governance processes and other cross office processes. Guidance is not appropriately reviewed or approved prior to release. Appropriate legal input is not sought.
- **Consultation and engagement -** Appropriate input is not sought from the expected audience and key external stakeholders for the guidance. External consultants, or legal advice is not sought where necessary
- **Guidance promotion -** Guidance is not delivered appropriately or effectively communicated to stakeholders, both internally and externally.
- **Measuring impact -** There is no method for collating and measuring the use and impact of published guidance. The impact and use of guidance is not monitored or evaluated.
- **Improvement process -** There is no improvement process in place for future published guidance.

The scope for the audit is concerned with assessing whether the ICO has in place adequate and appropriate policies, procedures and controls to manage the above risks. We will review the design of controls in place and, where appropriate, undertake audit testing of these to confirm compliance with controls, with a view to forming an opinion on the design, compliance with and effectiveness of controls. Testing will be performed on a sample basis, and as a result our work does not provide absolute assurance that material error, loss or fraud does not exist.

Definitions of Assurance Levels	
Level	**Description**
Substantial	The framework of governance, risk management and control is adequate and effective.
Adequate	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Limited	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.
Unsatisfactory	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

Definitions of Recommendations		
Priority	**Definition**	**Action required**
High	Significant weakness in governance, risk management and control that if unresolved exposes the organisation to an unacceptable level of residual risk.	Remedial action must be taken urgently and within an agreed timescale.
Medium	Weakness in governance, risk management and control that if unresolved exposes the organisation to a high level of residual risk.	Remedial action should be taken at the earliest opportunity and within an agreed timescale.
Low	Scope for improvement in governance, risk management and control.	Remedial action should be prioritised and undertaken within an agreed timescale.

Statement of Responsibility

We take responsibility to the Information Commissioner's Office (ICO) for this report which is prepared based on 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 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

Hannah Parker
Associate Director, Mazars
hannah.parker@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 44,000 professionals – 28,000 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