



Information Commissioner's Office

Internal Audit Report: Investigations & Enforcement
March 2021

mazars

Contents

01 Introduction	1
02 Background	1
03 Key Findings	1
3.1 Examples of areas where controls are operating reliably	2
3.2 Risk Management	3
3.3 Value for Money	4
3.4 Sector Comparison	4
04 Areas for Further Improvement and Action Plan	6
A1 Audit Information	9

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 A1 of this report for further information about responsibilities, limitations and confidentiality.

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 Investigations and Enforcement Action. We have reviewed key controls to assess whether the ICO's framework and processes are designed and operating effectively. This included the following risk areas:

- Methodology;
- Initial Prioritisation, Planning and Scoping;
- Monitoring and Decision Making;
- Enforcement Action and Approval Stages;
- Post Investigation Activity;
- Reporting; and,
- Future Proofing/Development.

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

We are grateful to the Director of Investigations, both Heads of Investigations Intelligence and other staff across the four Investigation Team areas, for their assistance during the audit.

The fieldwork for this audit was completed whilst government measures were in place in response to the coronavirus pandemic (Covid-19). Whilst we completed 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.

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

The ICO has both investigative powers and regulatory powers, which include taking enforcement action under the Data Protection Act (DPA) 2018 (and DPA 1998) and FOIA 2000. Authority in deciding whether to bring a prosecution is delegated to the designated lawyer(s) employed by the ICO. It is these lawyers who are the decision makers who exercise the delegated authority and who prosecute independently.

The ICO have an established Investigations Team that is responsible for investigating and enforcing any breaches of legislation the ICO regulates:

- Data Protection Act 2018 (DPA 2018);
- General Data Protection Regulation (GDPR);
- Privacy and Electronic Communications Regulations 2003;
- Freedom of Information Act 2000 (FOIA);
- Network and Information Systems Regulations 2018 (NIS); and
- Electronic Identification, Authentication and Trust Services Regulation (eIDAS).

Where necessary investigations may lead to issuing enforcement action, therefore the Investigation Team work closely with the ICO's Legal Team from an early stage to ensure legal consideration are made.


The Investigations Team is split into five specialist areas: Civil investigations; Criminal investigations; Cyber Incident Response; Privacy and Digital Marketing; and the Financial Recovery Unit. The scope of our work reviewed the specialist teams, excluding the Financial Recovery Unit.

The ICO has developed an overarching Investigations Manual which details the processes and procedures that are expected to be followed when investigating suspected infringements of data protection laws. The Investigations Manual also sets out the roles, responsibilities, and stages which all investigations should follow through to closure, including the interaction with the Legal Team.

The ICO are required to assess complaints and information shared with the Investigations Team before formally committing to proceeding to investigate. The Investigations Team will conduct a triage of the information, whereby each case is considered against the ICO's Strategic Priorities (IRSP Goals) and regulatory priorities and the principles set out in the Regulatory Action Policy (RAP). At the triage stage cases are also prioritised based on the risk and impact of the breach.

All Investigations are recorded and monitored through a Case Management System; Crimson. Crimson allows investigation actions to be reviewed and approved by Team Managers throughout the investigation. Updates are provided weekly within the four sub investigation teams and the Director of Investigations, with high-level reports issued monthly to the Senior Leadership Team (SLT).

03 Key Findings

Assurance on effectiveness of internal controls			
		Substantial Assurance	
Rationale			
<p>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.</p> <p>Our audit has identified one significant weakness in relation to a formal close out process and lessons learned. Overall, we feel that overall risks are being effectively managed. The other issues raised are minor areas for improvement within an adequate control framework. Please see Section 04 for further detail in respect of the recommendations made from our review.</p>			
Number of recommendations			
Priority 1	Priority 2	Priority 3	Total
-	1	2	3

3.1 Examples of areas where controls are operating reliably

- The ICO have established an overarching Investigations Manual which was last updated in September 2020. The Manual is details each stage of the investigation process, including 'how and why' key processes are to be completed.

Our review confirmed that the Investigations Manual sets out roles and responsibilities across the organisation, including cross-office working at respective stages. Additionally, The Manual sets out the process of prioritisation and the criteria of each of the five-category system developed to prioritise cases. The five categories are as follows:

- P1 – High risk/ impact;
- P2H – High risk/ medium impact;
- P2M – Medium risk/ high impact;
- P3 – Medium risk/ medium impact; and,
- P4 – Low risk/ low impact.

We reviewed the definitions and criteria as set out in the ICO's Investigations Manual and confirmed that the principles outlined are clear in what is expected to meet each priority status. The ICO ensure by use of examples that there is a separation of what is classed as a high risk or impact investigation.

- A Strategic Threat Assessment is performed annually by the ICO's Intelligence Department. This was last carried out in September 2020 (aligning with the Investigations Manual) and is developed to guide and drive the regulatory priorities for the forthcoming year; it is these regulatory priorities that are embedded as part of the prioritisation process for reviewing initial investigation information.

Our detailed sample testing of 12 investigations; three across each of the four teams, confirmed that each of the sampled investigations had been through the ICO's initial prioritisation process, ensuring alignment with the regulatory priorities and the ICO's Information Rights Strategic Plan.

- The ICOs investigation framework consists of five phases: scoping/planning; conducting the investigation; investigative outcomes; decisions; and, legal advice. Each of the stages and steps are required to be documented initially within a formal Investigation Plan, with ongoing case management updates recorded in Crimson. As investigations progress towards recommendation, formal outcome reports are documented to demonstrate rationale for the ICO's conclusions.

Actions are set by Team Managers in Crimson. These are "actioned" by Case Officers and reviewed by Team Managers once complete. New actions are then set as the investigation progresses, therefore enforcing appropriate review throughout. As part of Crimson review, Team Managers and Group Managers will continually assess the progress of investigations to ensure they are conducted in a timely and effective manner, per the Investigations Manual.

Our sample testing of the 12 investigations confirmed that all investigations were able to appropriately demonstrate review throughout the management of each investigation.

- As investigations conclude, recommendations must be made based on the investigation's findings. Recommendations are formally documented in Enforcement Action Outcome Reports which are required to be reviewed and approved prior to referral to delegated authorities. As part of the recommendation process, investigations may require formal meetings to take place to support the final recommendation. For instance; Decision to Impose Meetings (DTI) and Penalty Setting Meetings (PSM) may need to take place to make the appropriate regulatory decision on whether to issue a Monetary Penalty Notice (MPN) or an Enforcement Notice and what the terms and monetary amount should be.

Our review sample tested eight closed investigations to assess the effectiveness of recommendation decisions being reviewed and approved prior to formal Enforcement Action is taken. Our findings were able to confirm that each of the eight closed investigations appropriately demonstrated compliance with the Investigations Manual, with evidence of Regulatory Panel outcome decisions also documented to demonstrate thorough and effective management prior to final recommendations being made.

- Administrative law governs public bodies if they are carrying out public functions, which includes making decisions and a judicial review is the legal procedure by which decisions of a public body can be challenged. The ICO therefore ensure that the Legal Team are consulted on any relevant investigations. Additionally, at the

conclusion of an investigation, the Legal team are responsible for drafting Notices of Intent.

Using our sample of eight closed investigations, we confirmed that four of these required legal involvement and that in each of the four instances, the ICO were able to demonstrate that legal advice had been sought from the ICO's Legal Team, with evidence documented and traced to respective Enforcement Action Outcome Reports.

- In relation to future proofing and development opportunities, the ICO have a wealth of horizon scanning controls in place. For instance, there are dedicated media monitoring processes which highlight relevant articles that are discussed at weekly team meetings. Example of which were shared as part of this review.

Additionally, the ICO have an established tool called the 'Knowledge Service Team' which provide regular 'knowledge packs' which provide key updates on any legislative changes. Similarly, monthly Threat Assessments are produced and shared across the ICO by the Intelligence Team. These assessments include comparisons with the National Cyber Security Centre (NCSC) and law enforcement agencies, drawing on any trends and patterns. The assessments also help drive the annual Strategic Threat Assessments. Again, the ICO shared examples to demonstrate the ICO's adaptive approach.

3.2 Risk Management

There are a number of controls that feature across other closely linked strategic risks, for instance:

Risk 57 (R82) – *"If the ICO, in its role as a regulator, fails to deploy its powers in targeted, proportionate and effective way, there is a risk that our regulatory interventions will not achieve the change in behaviour needed to build public trust and confidence."*

Risk 9 (R61) – *"Litigation Resource: Risk that multiple or a single significant legal challenge or trend emerges (Threat) diverting significant financial and non-financial resources into possibly lengthy legal disputes, impacting upon the ICO's ability to legally defend itself which could have a domino effect on its decision making, its*

financial resilience, its reputation as an effective regulator and diluting its operational ability to achieve all of its IRSP goals.”

The following mitigating controls across both risks have been identified which relate to the scope of this review:

- Strategic Threat Assessment and Regulatory Priorities;
- Case triage system for referrals to Investigations;
- Delegated authority scheme in place to reduce pressure on key decision makers;
- Close links with enforcement team to review current and potential investigations

Based on our findings and observations we were able to confirm that each of the sampled investigations had been through the ICO’s initial triage process, which ensures that investigations align with the regulatory priorities and the ICO’s Information Rights Strategic Plan. However, we also identified that 122 Cyber cases had not yet been allocated to a Case Officer. Through discussion with management it was confirmed that this was due to a volume issue which had already been highlighted, with not all cases requiring formal investigation. Management also confirmed that the root-cause to this had been identified as the lack of expertise at the triage stage for Cyber cases, with action in-progress to resolve the issue.

A Strategic Threat Assessment is performed annually by the ICO’s Intelligence Department. This was last carried out in September 2020 and is developed to guide and drive the regulatory priorities for the forthcoming year; it is these regulatory priorities that are embedded as part of the triage process for reviewing initial investigation information.

Additionally, we were able to confirm that where enforcement action had been taken for our sample of closed investigations, legal advice had been sought and appropriately demonstrated.

3.3 Value for Money

Value for Money can often be difficult to derive in an investigatory or inquiry context due to the fact the nature of activity is extremely varied depending on the investigation at hand. For instance, investigations will vary in complexity as well as involvement of Policy, legislative or other requirements. The efficiency and effectiveness are also directly impacted

by the nature of what is being investigated and whether there are corresponding parties and external resources required to be involved. As a result, attempts to create efficiency savings increases the risk of possible failure, which could lead to reputational damage that may outweigh any potential savings created.

The use of case management systems can help to reduce the burden of manual monitoring and management of cases and progress. Such systems can offer functionality of storing information and forms to enable quicker review processes where possible. Our review confirmed that all four sub-investigation teams have recently moved over to the case management system; Crimson. Crimson is an investigation software solution designed to deliver a secure database for recording and investigating incidents. One observation we identified was that the ICO use Crimson and report templates to document progress of investigations when formulating recommendations. The ICO may wish to consider how Crimson can be used to generate reports to help achieve efficiencies.

The use of specialist staff increases the effectiveness of investigations, as it means there are multiple skills utilised, and reduces the cost requirements of relying on outside specialists if they are required. Provided there is enough work to fill their time, these provide a good source of value for money.

3.4 Sector Comparison

By comparing the equivalent of the investigation process to that of other regulators we work with, we have identified common themes of good practice across the sector. These include:

- Focusing resources on areas of greatest risk;
- A regime of continuous monitoring;
- Improved early identification, and the subsequent management, of issues;
- Continuous improvement driven by lessons learned reviews;
- Appropriate and timely revision to policies & procedures; and
- Proportionate engagement with partner agencies.

In relation to our assessment of the ICO’s control framework compared to those of the key themes from others within the sector, we have largely found that the ICO operative an effective control framework with strong

processes as we have seen elsewhere. There is however, one area for improvement we identified relative to the ICO's lessons learned processes. We have therefore put forward a recommendation to strengthen the ICO's performance in light of good practice we have reviewed elsewhere.

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	<p>Investigation Closure and Lessons Learned</p> <p><i>Observation:</i> The ICO currently do not have a formal closure process established which also considers lessons learned.</p> <p>Review of the Investigations Manual confirmed that a detailed expectation is documented for High Profile Investigations, however, there is no information or expectations established for investigations across the four sub-investigation teams; including how and when lesson learned should be carried out.</p> <p>Discussion with management confirmed that formal closure is demonstrated through Enforcement Action Outcome Reports or Investigation Outcome Reports, however any lessons learned are not formally documented or shared across the Investigations Team.</p> <p><i>Risk: The ICO do not have formal closure processes for investigations.</i></p> <p><i>Additionally, lessons are not learned from Investigations, leading to the ICO not realising any good or bad practice experiences that can develop current processes across the organisation.</i></p>	<p>The ICO should developed and document a formal investigation closure process, which includes lesson learned steps.</p> <p>We appreciate that the ICO is tasked with investigating large numbers of incidents, therefore the process should consider the viability of resources available and the necessity of which investigations require formal closure. For instance, investigation priority ratings or reputational impact of investigations are factored into the criteria for formal closure processes.</p>	2	<p>During Q1 2021-2022, we will review our current debrief and Enforcement Report process to introduce a proportionate process to identify and share lessons learned from case outcomes with relevant internal and external stakeholders.</p>	<p>Q1 21-22</p> <p>AC/HP (delegated to MS)</p>

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
4.2	<p>Investigation Plans</p> <p><i>Observation:</i> As part of our detailed sample testing, we reviewed 12 investigations; three across each of the four sub-investigation teams. This sample testing identified the following compliance issues against the ICO's Investigations Manual:</p> <ul style="list-style-type: none"> One investigation did not have a documented Investigation Plan and therefore was unable to demonstrate stages planning of the investigation or managerial sign off; and Two further investigations did not demonstrate managerial sign off of the Investigation Plan, albeit we further confirmed had that managerial sign-off had been evidenced in Crimson and had not been recorded on the Investigation Plans themselves (administrative issue). <p><i>Risk: Investigations are not appropriately planned, scoped, and resourced prior to commencement.</i></p>	<p>The ICO should ensure that all investigations have a documented and signed off Investigation Plans (or equivalent) prior to commencement of the investigation.</p> <p>The ICO may wish to explore the functionality within Crimson to assess whether Investigation Plans are necessary if equally effective records can be documented and approved within Crimson.</p>	3	<p>Group Managers undertake Quarterly audits of sample cases to check that compliance is being achieved with the processes in the Investigation Manual. Management advice is provided in cases where non-compliance is identified. In addition, regular reminders are issued at team meetings and in 1-1s to staff and managers about the importance of completing IPs.</p> <p>During Q1 21/22, we will review the functionality of Crimson to consider whether we can achieve the aims of the IP through the case management system.</p>	<p>Q1 21-22</p> <p>Crimson Management Group (MS)</p>
4.3	<p>Reporting</p> <p><i>Observation:</i> The ICO have various mechanisms for reporting investigation updates across the team and to Senior Management. We reviewed examples of reports and identified cross-over and duplication of reporting, with varying level of detail provided in each report, despite underlying</p>	<p>The ICO should perform a review of the current reporting arrangements and consider what information is necessary at each management level and whether efficiencies and high-level</p>	3	<p>There is an existing ICO project underway to introduce more relevant management information aligning it with the introduction of KPIs as part of a balanced scorecard approach. As part of that work, and while the audit was</p>	<p>Q1 21-22</p> <p>AC/HP</p>

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
	<p>messages being the same. For instance, the ICO have the following reports:</p> <ul style="list-style-type: none"> • Monthly Directorate Impact Reports which provide an engagement and influence update across each of the four teams; • Quarterly performance updates supporting the Information Rights Strategic Plan, providing general updates about investigation activity within the quarter; • Monthly Operations Summary Reports which require high-level updates in relation to investigation numbers; • Monthly Significant High-Profile Case Reports, providing an update on individual 'high-profile' investigations; and • Weekly Management Information 'Snapshots' which provide high level updates in relation to investigation numbers <p>Review of the Investigations Manual also identified that the ICO have not yet established a set of Key Performance Indicators to help provide a reflection of performance across the Investigations Team.</p> <p><i>Risk: The ICO's reporting processes are inefficient, possibly leading to insufficient reporting for decision making purposes.</i></p>	<p>summaries can be provided where no decision is required.</p> <p>The review should also ensure that Key Performance Indicators are considered at each reporting level and what performance detail is necessary at each level to inform decision making.</p> <p>This review should also consider enforcing consistent reporting approaches across the teams to aid escalation reporting for Senior Management.</p>		<p>ongoing, the Directorate has already contributed to the introduction of team-level KPIs and will include this information in its reporting, where appropriate.</p> <p>The nature of the Directorate's work means that there is a requirement for reporting on case progression to various senior management levels, some of which is inevitably duplicated.</p> <p>However, the Directorate management team will keep the requirement for MI under review and aim to reduce unnecessary duplication where it is identified. To that end, during Q1 2021-2022 we will review the current MI templates within the Directorate to reduce duplication and ensure consistency of reporting.</p>	

A1 Audit Information

Audit Control Schedule	
Client contacts:	Steve Eckersley – Director of Investigations Hazel Padmore – Head of Investigations Any Curry – Head of Investigations
Internal Audit Team:	Peter Cudlip, Partner Darren Jones, Manager Chris Hogan, Senior Auditor
Finish on site/ Exit meeting:	24 February 2021
Last information received:	10 March 2021
Draft report issued:	29 March 2021
Management responses received:	7 April 2021
Final report issued:	8 April 2021

Scope and Objectives

Audit objective: To provide assurance over the design and effectiveness of the key controls operating in relation to; the ICO's investigations and enforcement processes. Our review considered the following risks:

- **Methodology** – The ICO do not have a robust methodology and strategy for investigations, setting out roles and responsibilities. Investigations are progressed without any consideration of the ICO's Strategic Priorities and regulatory priorities.

- **Initial Prioritisation, Planning and Scoping** – Investigations are not appropriately prioritised, scoped or resourced prior to commencement.
- **Monitoring and Decision Making** – Investigations are not appropriately reviewed (including decisions on prioritisation, scope and resource) during the investigation. Investigation progress is not effectively monitored and reviewed. Decision making stages during investigations are not appropriately recorded or approved where applicable.
- **Enforcement Actions and Approval Stages** – There is insufficient managerial review of recommendations at the conclusion of an investigation. In cases which proceed for a decision on whether to take formal enforcement action, there are insufficient processes of review / approval of this recommendation prior to the matter being referred to the delegated authority. Legal advice or support is not provided in a timely / appropriate manner which supports cases proceeding to enforcement action.
- **Post Investigation Activity** – Investigations are not formally closed, reviewed and, where appropriate, visibility of outcome provided to other departments within the ICO. Lessons learned are not performed and shared across the ICO.
- **Reporting** – Senior management are not provided with sufficient information due to inadequate reporting of investigations.
- **Future Proofing/Development** - The ICO do not consider or adapt the investigations framework to anticipate future legislative or technological changes. For instance, intelligence information is not utilised to prepare for future demand.

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 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, 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.
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 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

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