



Information Commissioner's Office

Internal Audit Report: Stakeholder Management

November 2021

mazars

Contents

01 Introduction	1
02 Background	1
03 Key Findings	1
3.1 Examples of areas where controls are operating reliably	1
3.2 Risk Management	2
3.3 Value for Money	3
3.4 Sector Comparison	2
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 2021/21, we have undertaken a review of the Information Commissioner's Office (ICO) arrangements for stakeholder management within the Relationship Management Service (RMS). 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:

- Strategy;
- Risk Assessment and Profiling;
- High Risk Stakeholders;
- Supervision of Stakeholders;
- Supervisory Records;
- Reporting; and,
- Previous Recommendations.

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

We are grateful to the Director – High Priority Inquiries, Insight, Intelligence & Relationship Management, the Head of RMS & Insight and the Group manager for RMS for their assistance during the audit.

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

Approaches to, and methods of communicating with stakeholders depend on the aims of an organisation and the nature of those stakeholders. Stakeholders can support, challenge or oppose decisions or actions; however, it is vital that they are communicated with on an on-going basis and that relationships are maintained.

The ICO's Information Rights Strategic Plan 2017-21 ('IRSP') sets out six strategic goals for the organisation. Goal Two stipulates an ambition to 'Improve standards of information rights practice through clear, inspiring

and targeted engagement and influence across the organisation'. Whilst the ICO are awaiting the commencement of the new Information Commissioner, the 2017-21 IRSP strategic objectives remain.

In the financial year 2019/20, the ICO's Service Excellence Pack identified the need for a function to manage high risk stakeholders, which led to the creation of the Relationship Management Service (RMS). This function was designed with the remit of being the "co-ordinating point of contact for a portfolio of organisations that present the highest regulatory risk and present the most significant opportunities to influence the privacy landscape". In practice, stakeholder relationships are managed by various teams across ICO, dependent on expertise. For example, stakeholders such as Microsoft and Facebook will be managed by the Digital and Tech Team, whilst the RMS retain lead over some central government departments (the majority being managed through the Parliamentary and Government Affairs team) and some regulatory bodies such as OFSTED, Financial Conduct Authority, some representative bodies such as UK Finance, and also with bodies such as the Bank of England and the Metropolitan Police Service.

In 2020-21, we provided Limited Assurance on Stakeholder Management to the ICO. Since this review, the RMS function has undergone significant change; both its resource and its approach to stakeholder management. Namely, the RMS have established core stakeholder sectors rather than focussing individually on stakeholders. This categorisation into sectors came following feedback from stakeholders that they would value sectoral expertise, and identified risks of stakeholder engagement not being coordinated across the office on this basis. As such it was recognised that there would be value in the RMS mapping out and coordinating an overall picture of engagement for these specific sectors, established as follows:


- Health
- Financial Services
- Police and Justice
- Education

In addition to the RMS' sectoral approach, the ICO have adopted 'Medelow's Matrix' for analysing stakeholders. This is a change from the previous approach of assessing stakeholders based on risk. The four categories adopted based on influence and opportunity to the ICO, are:

- Keep Satisfied

- Manage Closely
- Monitor
- Keep Informed

03 Key Findings

Assurance on effectiveness of internal controls			
		Moderate 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 Moderate Assurance.</p> <p>Our audit has identified a number of significant areas for improvement in relation to: -</p> <ul style="list-style-type: none"> Developing an operating model or suite of procedures which sets out the ICO's detailed approach to stakeholder management; Establishing formal reporting mechanisms and performance indicators to be able to provide progress updates to management for decision-making purposes, and; Developing a high-level 'next steps' plan to outline the direction of travel for the RMS team and stakeholder management. <p>Overall, we feel that some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control. 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
-	3	-	3

3.1 Examples of areas where controls are operating reliably

- The ICO's RMS function has developed a Stakeholder Engagement Strategy, which was updated and presented to the Communications and Engagement Board in October 2021. The Strategy was updated significantly to reflect the change in stakeholder engagement approach of the RMS.

We reviewed the RMS Stakeholder Engagement Strategy and confirmed that the paper details the approach that to review engagement on a sector basis, with engagement analysis having been performed to determine which sectors to prioritise in the short-term.

We also confirmed that whilst the Information Rights Strategic Plan is due to be updated with the commencement of the new Information Commissioner, there is alignment to Strategic Objective 2: *"Improve standards of information rights practice through clear, inspiring and targeted engagement and influence"*.

- Sector Engagement Plans are reviewed and approved by Directors to ensure an organisational-wide assessment has been taken into consideration when establishing plans.

At the time of testing Sector Engagement Plans were in draft form, however, we were able to confirm each of the four established sectors; Health, Financial Services, Police and Justice and Education, that PESTLE analysis, sector and ICO regulatory priority mapping, and key objectives had been developed for each.

- In relation to stakeholder supervision and supervisory records, all current engagements with stakeholders are recorded in Stakeholder Profiles. Communication, particularly briefing notes, are recorded on the ICO's SharePoint.

We sample tested 12 of RMS' key stakeholders covering each of the four established sectors and ranging across each of Mendelow's four categories. We confirmed that ten of the 12 were able to appropriately demonstrate evidence of engagement as documented in respective Stakeholder Profiles. We subsequently traced each of the ten instances through to SharePoint to confirm recording.

The two instances where evidence had not been provided were confirmed by management that both Stakeholder Profiles had yet to be updated to align with the draft Sector Engagement Plans. We have referenced this within recommendation 4.3.

- With regard to previous recommendations from the Limited Assurance report in 2020/21, our follow-up report presented to Audit Committee in June 2021 confirmed the four recommendations included had been evidenced and closed as implemented.

3.2 Risk Management

The ICO's Corporate Risk and Opportunity Registers do not make explicit reference to the established RMS, however, the following mitigating controls have been identified within other risks in relation to stakeholder management and engagement:

R85 – Managing ICO Reputation

Mitigating control: High-level engagement strategy agreed across RMS, PGA, Communications. Actions being implemented on an iterative basis.

R88 – Future role and structure of the ICO

Mitigating control: completion of stakeholder engagement plan for targeted engagement.

R87 – International position

Mitigating controls: Ongoing engagement with Norwegian DPO re LSA status in IBO exam approach, and; monthly engagement with DCMS, DIT, FCDO and HO via Senior International Contact Group.

Our review of stakeholder management in 2020/21 confirmed that the RMS function at the time maintained its own risk register with specific risks relation to the RMS' ability to deliver its intended outcomes. However, during this review, we identified that the RMS function no longer maintains a risk register.

Whilst we would not expect a specific strategic risk to be established in relation to stakeholder management, the ICO should consider developing an operational risk in order to ensure any residual risk is monitored. We have raised a recommendation in relation to this in Section 04.

3.3 Value for Money

Value for Money can often be difficult to derive in a stakeholder management context due to the fact the nature of activity is extremely varied depending on the stakeholder and respective sector. The efficiency and effectiveness are also directly impacted by the nature of legislation and whether there are joint engagement pieces with multiple parties 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.

Poorly managed stakeholder relationships can have a significant impact (both in terms of staff time and financial outlays) on the achievement of value for money. Efficiently and effectively managed engagements by contrast should result in the achievement of key objectives which ultimately improve processes or activities and contribute to improved overall value for money. Implications also arise through any associated resources and administrative systems underpinning relationship management within the organisation such as a dedicated Customer Relationship Management (CRM) system or equivalent.

The use of CRM can help to reduce the burden of manual monitoring and managing cases and progress. Such systems can offer functionality of storing information and forms to enable quicker review processes where possible. Our review identified that the RMS function use the ICO's SharePoint system as a repository for all and any stakeholder engagements. The ICO's SharePoint is a basic system with limited functionality and management confirmed that uploading documents can be a time-consuming process. The ICO should therefore consider performing a cost benefit analysis to determine whether a dedicated CRM system would be value for money.

3.4 Sector Comparison

Every organisation has different stakeholders and priorities in regard to engagement. However, the core processes required to accomplish this are broadly similar. The ICO has updated its processes to reflect the sectoral approach to engagement across the organisation. This update in approach is based on the organisation's overall strategic goals, which implicitly

require effective engagement with stakeholders and optimising on opportunities that occur across key sectors.

The main barrier organisations find with stakeholder engagement is overcoming the 'silo effect' of different departments, which can impact on the consistency of message, focus and co-ordinated approach. The numerous work streams across ICO, such as the RMS, Business Services, Digital, Tech & Innovation and High-Profile Investigations Teams, means the likelihood of overlap with stakeholders is high. We have noted that the RMS' change to a more sectoral approach is a step in the right direction to mitigate such risks. At other clients we see that some of these issues can also be alleviated through the use of a CRM system, as detailed in our VfM section. However, this also requires a consistent use of the system across the entire organisation to achieve this effectively.

Across our client base it is typical to see areas of training and guidance provided on stakeholder engagement. This helps to ensure a consistent approach is applied and that individuals across the organisation are clear about who to engage with and which form of communication to use. Furthermore, at other organisations we often see the creation of a long-term stakeholder engagement strategy, aligned to the organisation's corporate strategy. The strategy details information such as the organisations key stakeholders, methods for communication, and milestones for progress which are reviewed continuously. Given the recent change in Commissioner at the ICO, the RMS function should ensure that any subsequent updates to the IRSP are reflected within the stakeholder management strategy and guidance is communicated across the Office.

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>Stakeholder Engagement Operating Model</p> <p><i>Observation:</i> The ICO's RMS function has established a high-level Stakeholder Engagement Strategy which was presented and approved by the Communications and Engagement Board in October 2021.</p> <p>Our review of the overarching strategy identified that operational level details are not included. Whilst we would not expect an overarching strategy to include operational detail, the ICO do not have any supporting procedure or process notes highlighting operational detail. For instance, we expect the following examples of operational detail to be provided:</p> <ul style="list-style-type: none"> • how stakeholders are assessed and categorised using Medelow's Matrix – the rationale, approval and what criteria determines positioning in each of the four categories; • how often Sector Engagement Plans are to be assessed; and • roles and responsibilities for each key procedure. <p>We further identified a lack of operational detail around the ICO's expectations for each of Mendelow's categories, and how these</p>	<p>The ICO should develop a detailed operating model aimed to set out all operational activity in relation to stakeholder engagement. The operating model should include:</p> <ul style="list-style-type: none"> • how stakeholders are assessed using Mendelow's Matrix, • roles and responsibilities, including Director involvement and details of stakeholder escalation routes, • how sector engagement plans should underpin individual stakeholder profiles, • the expected content of what stakeholder profiles should include; the desired outcomes and impact of our engagement and routes to achieving this. • frequency of reviewing Sector Engagement Plans and Stakeholder Profiles, • utilisation of intelligence across the office to support stakeholder assessment and 	2	<p>An operating model will be prepared, at an appropriate level of detail, and shared across the organisation. This will include how we engage with other parts of the organisation, and clarity on roles and remit with regard to stakeholder engagement.</p> <p>We will review the content of our draft sector engagement plans, taking into account auditor feedback.</p> <p>Our sector engagement plans will be amended to include explicit reference to roles and escalation routes, taking into account the emerging new ways of working across different sectors (i.e. the finance hub, and potential health hub).</p> <p>Sector engagement plans will be signed off by the relevant director and executive director, and be shared and published internally</p>	<p>The documented operating model will be developed by end March 2022 to support the 2022/23 business plan.</p> <p>Quarterly reviews will take place during 2022/23</p> <p>Christina Barnes</p>

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
	<p>subsequently underpin individual stakeholder profiles. This includes what escalation mechanisms are established should issues or key intelligence need to be shared across the organisation.</p> <p><i>Risk: Stakeholder engagement arrangements are unclear, with lack of detail around roles and responsibilities of the RMS function and the wider office, leading to inconsistent or insufficient engagement with key stakeholders.</i></p>	<p>movement between Mendelow's Matrix categories, and</p> <ul style="list-style-type: none"> frequency and details for reporting progress against objectives 		<p>Sector engagement plans will be reviewed quarterly, and between this quarterly review, escalation will occur by exception.</p>	
4.2	<p>Reporting</p> <p><i>Observation:</i> The ICO's RMS function and Stakeholder Engagement Strategy has not established any performance indicators or reporting arrangements to support the evaluation of performance and progress of the RMS' objectives.</p> <p>Within the RMS' Stakeholder Engagement Strategy it states, "<i>RMS will develop clear management reports to ensure we develop and build effective performance reporting measures which can be used as the basis of measuring success.</i>" However, as identified above, no reporting arrangements had been developed at the time of testing.</p> <p>Discussion with management confirmed that they are aware that work needed to be done on reporting and that the intention is that reporting will focus on sectoral updates and by exception for individual stakeholders of concern or of high-profile.</p> <p><i>Risk: The ICO do not report stakeholder management performance information for key decision-making purposes, leading to management</i></p>	<p>The ICO should establish a set of key performance indicators in relation to stakeholder management. The KPIs should align to the strategy's vision and wider corporate objectives, with consideration on impact of engagement work to allow management to make key decisions where necessary.</p> <p>Additionally, the RMS function should consider reporting lines both within RMS and the wider ICO, particularly for high-influence stakeholders.</p>	2	<p>Overarching KPIs for RMS will be set out within the forthcoming 2022/23 business plan.</p> <p>Each sector plan will have it's own KPIs and these will be reviewed quarterly</p> <p>Reporting lines for each sector will be clearly set out in the sectoral plans.</p> <p>A management report will be presented to the Executive Director on a monthly basis reviewing the overall performance of RMS.</p>	<p>End April 2022</p> <p>Christina Barnes</p>

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
	<i>being unaware of any key performance issues or failure to meet engagement objectives.</i>				
4.3	<p>RMS Next Steps</p> <p><i>Observation:</i> The RMS Stakeholder Engagement Strategy is still in its infancy. Following review of the Strategy, we identified that there is a high-level plan of next steps to operationalise objectives.</p> <p>The high-level plan states that <i>"for some key organisations, RMS will retain ownership of their relationship with the ICO and will proactively engage with. These are organisations who whilst outside of a core sector still have present significant risk or have potential for helping us achieve impact. For others they will be able to engage with the ICO through our helplines, or through other contacts across the ICO."</i></p> <p>However, the Strategy does not address how these stakeholders outside the four established sectors will be reviewed, or how intelligence will help drive processes for assessing pipeline stakeholders.</p> <p>Additionally, during our sample testing of Stakeholder Profiles, we identified two profiles that were not up to date. Discussion with management confirmed that Stakeholder Profiles have yet to be updated to align with Sector Engagement Plans. Once Sector Engagement Plans have been ratified and finalised, individual profiles will subsequently be updated to reflect the RMS' sectoral approach to stakeholder management.</p> <p><i>Risk: Medium to long-term planning and of all stakeholders is inadequate, leading to ineffective</i></p>	<p>The RMS Stakeholder Strategy should build on the current high-level plan and establish clear next steps for how the RMS function will consider wider stakeholders and regular review of current high-influence profiles which fall outside the four developed sectors.</p>	2	<p>Wider review of stakeholders is dependent on forthcoming recruitment, as these stakeholders will be managed by new staff.</p> <p>Currently gathering evidence on who we engage with/need to engage with.</p>	<p>Initial review by endMay 2022</p> <p>Full review by end August months into, once new starters in place and understanding of RMS capacity to support additional stakeholders.</p> <p>Christina Barnes</p>

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
	<i>stakeholder awareness and management of all stakeholders.</i>				
4.4	<p>Operational Risk</p> <p><i>Observation:</i> The ICO's Corporate Risk and Opportunity Registers do not make explicit reference to stakeholder management and the established RMS function.</p> <p>Additionally, our review of stakeholder management in 2020/21 confirmed that the RMS function, at the time, maintained its own risk register with specific risks relation to the RMS' ability to deliver its intended outcomes. However, during this review for the year 2021/22, we identified that the RMS function no longer maintains a risk register.</p> <p><i>Risk:</i> Risks relating to the RMS' ability to deliver its intended outcomes are not identified and managed.</p>	Whilst we do not expect a strategic risk to be established relating to stakeholder management and we acknowledge that a specific risk register is best practice, the ICO should develop an operational risk in order to ensure any residual risk is monitored.	3	A full risk register will be developed for RMS to fit with business plan 2022/2023	<p>End April 2022.</p> <p>Christina Barnes</p>

A1 Audit Information

Audit Control Schedule	
Client contacts:	Anthony Luhman - Director – High Priority Inquiries, Insight, Intelligence & Relationship Management Christina Barnes - Head Relationship Management Service & Insight Natasha Andrews - Group Manager Relationship Management Service
Internal Audit Team:	Peter Cudlip, Partner Darren Jones, Manager Chris Hogan, Senior Auditor
Finish on site/ Exit meeting:	22 October 2021
Last information received:	27 October 2021
Draft report issued:	22 November 2021
Management responses received:	21 December 2021
Final report issued:	4 January 2022

Scope and Objectives

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

- **Strategy** – The ICO's RMS strategy for stakeholder management is not fit-for-purpose and does not align to the Information Right Strategic Plan.
The strategy does not make clear; roles, responsibilities and objectives of what they set out to achieve.
- **Risk Assessment and Profiling** – Risk assessment and profiling of RMS stakeholders is inadequate.
The ICO do not have mechanisms in place to capture information which may impact the risk rating of stakeholders.
- **High Risk Stakeholders** – The risk register for all high-risk RMS stakeholders is not monitored and maintained regularly.
- **Supervision of Stakeholders** – The ICO do not appropriately supervise high risk stakeholders to support the development and management of mitigating risk.
High risk stakeholders are not monitored regularly.
- **Supervisory Records** – Supervisory and relationship management services provided are not appropriately recorded and updated, leading to conflicting management of high-risk stakeholders.
ICO staff are not aware of the risk rating of RMS stakeholders.
- **Reporting** – The ICO do not report or escalate stakeholder management performance for key decision-making purposes.
- **Previous Recommendations** - Recommendations made in the previous stakeholder management review have not been implemented.

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:	The framework of governance, risk management and control is adequate and effective.
Moderate Assurance	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Limited Assurance:	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 Assurance:	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	Description
Priority 1 (Fundamental)	Significant weakness in governance, risk management and control that if unresolved exposes the organisation to an unacceptable level of residual 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, re-interpretation 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