MAZARS

ico.
Information Commissioner's Office

Internal Audit Report
Stakeholder Management
October 2020

Contents

In the event of any questions arising from this report please contact Peter Cudlip, Partner (peter.cudlip@mazars.co.uk) or Darren Jones, Manager (darren.jones@mazars.co.uk).

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 work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, We 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 of the Information Commissioners Office (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 stakeholder management, with a primary focus on the Relationship Management Service ('RMS'). We have reviewed key elements within the process to ascertain whether processes and controls are designed and operating effectively. This included risks in the following areas:

- Strategy and Handbook;
- Risk Assessments and Profiling;
- High Risk Stakeholders;
- Supervision of Stakeholders;
- Supervisory Records; and
- Reporting

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

We are grateful to the Interim Head of Compliance and Relationship Management, Director of High Profile Investigations & Intelligence, Group Manager of High Priority Investigations & Intelligence and other ICO staff for their support during the course of this audit.

The report summarises the results of the internal audit work and, therefore, does not include all matters that came to our attention during the audit. 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 coronavirus pandemic (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

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 on an on-going basis and that relationships are maintained.

The ability to effectively identify and engage with key stakeholders is essential for any organisation to ensure a good reputation is maintained and support is provided when needed from key groups. This is particularly important to ICO due to its prominent status and the nature of its work.

ICO's Strategic Goals – Stakeholder Management

ICO's Information Rights Strategic Plan 2017-21 ('IRSP') sets out six strategic goals for the organisation during the specified time period. Goal 2 stipulates an ambition to 'Improve standards of information rights practice through clear, inspiring and targeted engagement and influence' across the organisation.

In pursuit of these strategic goals, ICO's Service Excellence Pack (2019/20) identified the need for a function to manage high risk stakeholders, which led to the creation of the Relationship Management Service. 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" maintaining "overall oversight".

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 central government and regulatory bodies such as OFSTED, Financial Conduct Authority, the Bank of England and the Metropolitan Police Service. ICO's full schedule currently consists of 96 stakeholders.

Risk Assessments and Profiling of Stakeholders

Requests for ICO engagement are screened by the RMS weekly. If the RMS feel that the organisation is a potential stakeholder that aligns with the IRSP, then the assigned lead will conduct a risk assessment and high-level profile of the organisation and its data processing activities. Stakeholders are graded on the following bands, which determine the nature of the engagement, and the frequency of contact:

- Level 1 - High Risk / High Impact
- Level 2 – High Influence / High Impact
- Level 3 – Medium Risk / Medium Impact

Stakeholders can also be withdrawn from the schedule, should it be determined that it is no longer in line with ICO's or the stakeholder's strategic priorities to maintain a relationship.

Supervision of Stakeholders

Designated RMS leads are responsible for the overall vision and objectives of individual relationships with stakeholders. They are also responsible for the frequency and nature of contact during the engagement. All L1/L2 stakeholders are also assigned Executive Team (ET) or Senior Leadership Team (SLT) leads in order to oversee.
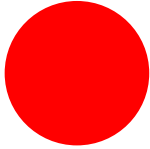
Each stakeholder's profile should be supported by an engagement plan, setting out objectives, timeframes and identifying alignment between their strategic priorities and that of ICO, as well as records of contact such as emails. Data is retained on SharePoints across ICO, but there is currently not a central relationship management system in operation.

Internal Performance Reporting

It is intended that the RMS will report internally to the Communication and Engagement Board, however, this has not happened to date. ICO has currently not identified any performance indicators for the RMS to report

against, and this lack of direction may have a resulting effect on the scope and outputs of stakeholder engagements.

03 Key Findings

Assurance on effectiveness of internal controls	
	Limited 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 **Limited Assurance** on the design and operation of controls within the Relationship Management Service.

Whilst there is a framework in place, our work has indicated that there are fundamental gaps and weaknesses in its operation.

We found that where key controls were listed in the RMS Strategy, there was often no clear, documented process of these being followed. This restricted our ability to accurately test the control's operation, and in some cases, there was no supporting evidence at all. We have included recommendation in Section 04.

Priority	Recommendations
1. (Fundamental)	2
2. (Significant)	2
3. (Housekeeping)	-
TOTAL	**4**

Areas of Strength

- The rationale behind the RMS function has clear links to the Information Rights Strategic Plan (2017-21) and places an emphasis on the importance of managing stakeholder relationships.

- The concept of centralising relationship management is efficient, and when utilised effectively can realise Value for Money.

- Organisation profiles can provide key strategic oversight of stakeholders, and effectively constructed engagement plans can allow for insight as to how stakeholder activities align with ICO's IRSP.

Risk Management

ICO's Corporate Risk and Opportunity Register does not make explicit reference to the RMS, however the following risks relate to communication with stakeholders:

R41 – Policy guidance is not responsive to external developments and stakeholder needs.

R44 – That the ICO fails to take advantage of opportunities to communicate our key messages to the public, to stakeholders and to new audiences.

Further actions identified include:

- Development of the planning grid and other mechanisms to ensure we have communication plans for all work;
- Embed new triage and prioritisation processes; and
- Development of stakeholder mapping work to better align comms and engagement activity with business priorities.

We believe that the RMS would be a key control to include within the above risks. Whilst the team's creation indicates an awareness of the need to coordinate and align stakeholder engagement, the current practices at ICO have weaknesses and inefficiencies that restrict RMS' effectiveness.

The RMS currently maintains its own risk register, the three highest perceived risks are:

010 (RAG 16) - Three tiers of management are all interim roles. Management key man dependency risk - Lack of effective oversight and management of the RMS is likely to have an impact on its ability to function, the competency of its team and its ability to have effective governance controls in place. There is also a potential for there to be an accountability risk.

001 (RAG 15) - Lack of required experience and competency in RMS. As half of the team are relatively new to the ICO and depth of experience with engagement and knowledge of the legislation vary significantly so this could have an impact on the effective operation of the team.

009 (RAG 12) - Lack of buy-in and proactive engagement from internal departments within the ICO and/or external stakeholders that RMS are attempting to work with. This could have a significant impact on RMS' ability to achieve its intended outcomes including reporting back to senior management.

We noted that the RMS Risk Register does not monitor residual risk and a distinction between completed and future actions identified to mitigate risk.

Value for Money

Improperly 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 system or equivalent.

Having a stakeholder relationship management framework helps to ensure value for money is achieved as it structures engagement processes, standardising processes whilst allowing flexibility to cater for the needs of individual stakeholders.

Sector Comparison

Every organisation has different stakeholders and priorities in regard to engagement. However, the core processes required to accomplish this are broadly similar. ICO has a tailored, reactive process based loosely on the organisation's overall strategic goals, which implicitly require effective engagement with stakeholders and optimising on opportunities that occur.

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 at other clients that some of these issues can 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. It was noted that this was an issue across ICO, as the current process is not utilised cohesively within the RMS and therefore a recommendation has been raised relating to this in **Section 04**.

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.

04 Areas for Further Improvement and Action

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

We identified a number of 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.

#	Observation/Risk	Recommendation	Priority	Management Response	Timescale/ responsibility
4.1	**Stakeholder management 1** Observation: The RMS Strategy states that the "RMS will be responsible for managing the relationship, co-ordinating office wide engagement in respect of all our stakeholders". However, through interviews with key staff members including Senior Policy Officers, we understand that in practice the RMS do not have oversight of all ICO stakeholders and the creation of their profiles and engagement plans. We also noted that the RMS has not carried out an overall review of stakeholders to: • Understand their profile level and whether this is still appropriate. • Ascertain whether the responsible lead is still appropriate. We noted four stakeholders (from our sample of ten) that had at least three assigned leads. • Check and understand the frequency of contact and whether all ongoing work across the ICO for stakeholders is recorded	The ICO should: • Clarify the remit of the RMS; • Ensure that the RMS coordinates all stakeholder relationships, they should ensure the RMS are involved in the onboarding and profiling of all future stakeholders, irrespective of their level of involvement during the subsequent engagement; • Carry out a review of all high-risk current stakeholders, to ensure that they are aligned with the IRSP and that they are assigned appropriate leads. • Regularly check that frequency of contact with stakeholders is recorded and appropriate.	1	ACCEPTED however we will need to consider more widely what co-ordinating all relationships will look like in practice. This will be picked up in a wider programme of work as part of the new engagement strategy.	April 2021 for the wider piece of work on co-ordinating all relationships. January 2021 to have undertaken the other recommendations

#	Observation/Risk	Recommendation	Priority	Management Response	Timescale/ responsibility
	Risk: Stakeholder management is ineffective leading to poor communications or issues with stakeholders.				
4.2	**Stakeholder management 2** Observation: The RMS strategy and manual set out a number of requirements for stakeholder engagement across ICO. We sought to test RMS engagement with ten high-risk stakeholders. During our testing, we noted the following: • For all ten organisations, scopes did not specify clear objectives, deliverable outcomes or clear timeframes for the relationship. There was also no evidence of approval of the scope; • For all ten organisations, we could not evidence the risk assessment completed at the initial screening or any approval; • Three organisations did not yet have an engagement profile. Of the seven organisations that had a profile, 5 did not have a documented engagement plan and therefore we could also not demonstrate alignment between their objectives and the IRSP. • For five the frequency of contact was either not recorded or unclear. There was no overall organisation profile in	The ICO should ensure full documentation is completed and retained for all key stakeholders. This should include: • Engagement plans and scopes that detail the objectives, frequency and relationships of the engagement; • Risk assessments including any mitigations and actions linked to the engagement plan; • Engagement profiles that detail key information of the stakeholders; • Organisation profile that detail all ongoing work across the ICO including the type of work, key contacts and dates.	1	ACCEPTED	JANUARY 2021

#	Observation/Risk	Recommendation	Priority	Management Response	Timescale/ responsibility
	place that should record ongoing work across all the ICO. Overall, for three stakeholders in our sample no documentation was provided to support stakeholder management. For a further three only the engagement profile of the stakeholder was provided. *Risk: Stakeholder management is ineffective leading to poor communications or issues with stakeholders.*				
4.3	**Escalations** Observation: Stakeholder leads are responsible for instigating escalations when issues arise; within the RMS, this would be the responsibility of Senior Policy Officers. Following identification of an issue there is no process in place for how to escalate an issue, should one arise. We do understand that there has been no previous requirement for escalations of issues with stakeholders, however, as noted in recommendation 4.2, record management for stakeholder communication is weak and therefore it is not possible to determine whether this is the case. *Risk: Issues at high risk stakeholders are not reported resulting in increased risk to the ICO.*	ICO should put in place a process for the escalation of issues that arise in stakeholder engagements.	2	ACCEPTED	DECEMBER 2020

#	Observation/Risk	Recommendation	Priority	Management Response	Timescale/ responsibility
4.4	**Internal Reporting on RMS** Observation: One of the three aims of the RMS included in their strategy is to '*Produce MI and report into the Communications and Engagement Board*'. We understand that no formal reporting has taken place since the team's creation in 2019. Nor has any formal performance evaluation of the RMS taken place as a whole. There are also no formally agreed performance indicators for the RMS. *Risk: The ICO do not report or escalate stakeholder management performance for key decision-making purposes and therefore have little or no understanding of communications and key issues across the key stakeholder group.*	ICO should agree and formalise: • Reporting and performance indicators for stakeholder management. • Reporting frequencies for the performance of RMS and any wider applicable teams.	2	ACCEPTED	DECEMBER 2020

A1 Audit Information

Review Control Schedule	
Client contacts:	Meagan Mirza, Interim Head of Compliance and Relationship Management

Anthony Luhman, High Profile Investigations & Intelligence |
| **Internal Audit Team:** | Peter Cudlip, Partner

Darren Jones, Manager

Matt Bell, Internal Auditor |
| **Exit Meeting:**
Last information received: | 1 October 2020 |
Draft report issued:	19 October 2020
Management responses received:	28 October 2020
Final report issued:	29 October 2020

Scope and Objectives

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

- The ICO's newly developed strategy and handbook for stakeholder management are not fit-for-purpose and don't align to the Information Right Strategic Plan. Neither the strategy or Handbook make clear; roles, responsibilities and objectives of what they set out to achieve.
- Risk assessment and profiling of all stakeholders is inadequate. The ICO do not have mechanisms in place to capture information which may impact the risk rating of stakeholders.
- The risk register for all high risk stakeholders is not monitored and maintained regularly.
- 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 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 stakeholders.
- The ICO do not report or escalate stakeholder management performance for key decision making purposes.

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 of, compliance with and effectiveness of internal 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.

MAZARS