Information Commissioner's Office

Internal Audit Report: Risk Management

February 2023

FINAL REPORT

Contents

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) risk management processes. Full details of the risks covered are included in **Appendix A1**.

It was agreed with the Director of Corporate Affairs and Governance that this audit will focus on the Corporate Risk Register and directorate Risk Registers. This audit has not reviewed and tested project/programme Risk Registers.

We are grateful to the Director of Corporate Planning, Risk &Governance, Head of Planning, Risk & Governance, Senior Corporate Governance Manager, Risk and Business Continuity Manager, Corporate Governance & Secretariat Group Manager and Corporate Governance Officer, along with 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

Risk management has been defined by the Institute of Risk Management (IRM) as, 'the systematic process of understanding, evaluating and addressing risks to maximize the chances of objectives being achieved and ensuring organisations, individuals and communities are sustainable'. Effective risk management is essential for all organisations in fulfilling their strategic goals. With the impact that Covid-19 and geopolitical instability has had on organisations, effective risk management has never been more important. Economic and political uncertainty, as well as emerging sector risks, has meant that organisations have had to rethink their business models and evaluate their current business risks and consider those moving forward in a 'new way of working'.

Risk management at the ICO is governed by the Risk Management Policy and Appetite Statement, which is supported by a Risk and Opportunity Management Procedure and 'Escalation and de-escalation' process document. The ICO's new strategy, ICO25, was published and became live in November 2022, replacing the previous Information Rights Strategic Plan (IRSP). The current Risk Management framework is aligned to the IRSP and the Risk and Governance department are in the process of realigning the framework to the new strategy.

Roles and responsibilities for all staff are set out in the Risk and Opportunity Management Procedure. The ICO have nominated Risk Champions from each directorate. The ICO created a role for a Risk & Business Continuity Manager, who has been in post since March 2022. However, due to staff sickness within the ICO, the Manager has been backfilling other roles and therefore has not been in post full-time.

Risk appetite statements are included in the Risk Management Policy and Appetite Statements document. The ICO does not have an overarching risk appetite statement, instead setting 22 appetites across its range of activities, reflecting the differing acceptance of various risks in achieving strategic priorities and outcomes.

Risk maturity was last assessed by the ICO in June 2019. The conclusion of this assessment was that the ICO defined their risk maturity as "risk defined" with an aim to move to being "risk managed" in the medium term.

The ICO's current risk reporting structure consists of:

- An overarching Corporate Risk and Opportunities Register (CRR) which is reported to the Risk and Governance Board (RGB) every six weeks and the Audit and Risk Committee quarterly. There are regular updates to Management Board with an annual deep dive
- Several directorate Risk Registers, accompanied by directorate Business Plans.

Risk scoring consists of combining an assessment of the likelihood (probability) of an event occurring, and its consequence (impact) on achieving the objective. Scoring of risks at the ICO is based on a 5x5 grid, with 25 being the highest and 1 being the lowest score available. Risks are scored as gross (without any treatment), net (with existing treatment) and target (once all treatments have been completed). The CRR scores are moderated via the Risk and Governance department and challenged at the Risk and Governance Board and the Audit and Risk Committee. Directorate risk scoring is moderated and challenged on the top three risks from each register by the Risk and Governance department.

Risks within registers are assigned owners, who are also responsible for the listed mitigating actions. The ICO's Intelligence Team conduct an annual Strategic Threat Assessment which is used to inform horizon scanning in relation to risk management.

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. Our audit has identified two key improvement areas: • Aligning the new ICO25 Strategy with the risk management framework; and • Ensuring directorate risk registers are complete and accurate. Please see Section 04 for further detail in respect of the recommendations made from our review.

Number of recommendations			
High	Medium	Low	Total
-	2	4	6

3.1 Examples of areas where controls are operating reliably

- Risk management at the ICO is governed by the Risk Management Policy and Appetite Statement. We confirmed that this document was reviewed and approved by the Audit and Risk Committee in January 2023. The Policy highlights a number of elements in relation to risk management and defines the ICO's risk appetite. As part of the review, we compared the ICO's Risk Management Policy to that of other organisations and identified some minor areas which could be improved or enhanced. These areas are highlighted in **Section 04.**
- The Policy is supported by a Risk and Opportunity Management Procedure, last reviewed by the Risk and Governance department in July 2022. The procedure document defines roles and responsibilities, sets out the ICO's approach to risk identification and assessment, scoring, treatment, monitoring and reporting. Roles and responsibilities are defined from the Commissioner to all staff.
- Risk appetite statements are included in the Risk Management Policy and Appetite Statements document. These statements are reviewed and approved annually by Risk and Governance Board (18 January 2022); and Management Board (21 March 2022). Most recently, the policy document was approved at the January 2023 Audit and Risk Committee.
- The Risk and Governance department developed a Risk Appetite Knowledge Pack to encourage the embedding of risk appetite. This is available to all staff via the intranet and has been presented by the Risk and Governance department to teams across the organisation.
- The ICO have delivered risk management training to the project manager group to increase awareness of risk management within key teams responsible for managing risk.
- We reviewed Terms of References for the Information Risk and Governance Group, Risk and Governance Board (RGB) and Audit and Risk Committee and confirmed that each contained adequate reference to risk and outlined each group's role in risk management. For example, the Terms of Reference for the RGB highlights that its role is to 'assist with the governance of the organisation and management of risk to achieving its strategic priorities and service delivery.' The RGB does this by reviewing and overseeing activity to develop and maintain the risk framework. The RGB also oversees monitoring and reporting arrangements.
- The ICO undertakes 'deep dives' periodically into selected risk areas in order to understand the potential likelihood, impact and controls in

more detail. Recently, a deep dive was competed on reputation risk. This was reported to the Risk and Governance Board in July 2022. The report highlighted 14 Corporate Risks that have interdependencies with reputation risk and the effects any changes in scoring would have on reputation risk.

- The Corporate Risk and Opportunities Register (CRR) currently contains 12 corporate risks. This is in line with what we see at peers, with best practice considered between 10-15 risks, allowing the ICO the focus efforts to the key risks impacting the achievement of its corporate objectives. All corporate risks have an owner, risk appetite, overall priority score, last reviewed date and next review due date. We reviewed assigned risk owners on the CRR which included Directors, Heads of Departments and Managers and deemed these to be appropriate on all occasions.
- Each risk on the CRR has a gross and current score reflected, as well as mitigating controls. Scores of each corporate risk are reduced after the application of mitigating controls, indicating successful risk treatment. *(N.B., We have raised a recommendation regarding scoring of risks in relation to the directorate Risk Registers in Section 04 below).*
- We confirmed, through review of minutes for the last 12 months, that the CRR is reported through Audit and Risk Committee quarterly with Management Board oversight. We reviewed minutes from the three Audit and Risk Committees (April 2022, June 2022 and October 2022) and confirmed that an update on the CRR and risk management was provided on all occasions. We confirmed that there was detailed discussion, scrutiny and challenge on risk on all occasions.
- We reviewed minutes from the last three Risk and Governance Board (August 2022, September 2022 and November 2022) and confirmed that an update on the Corporate Risk Register was provided on all occasions including any changes to scoring.
- The ICO has an escalation and de-escalation process in place for risks. Risks should be escalated or de-escalated, depending on the seriousness of their impact on the ICO, the achievement of objectives, the risk appetite and the risk score. The process also sets out the main triggers for escalating or deescalating a risk.

3.2 Risk Management

There are no risks recorded on the CRR which specifically relate to this audit area, which is common across the sector. Risk management is a core function and will naturally underpin the CRR, so we would not expect this to be a discrete area on the register. Our review has focused on the risks and areas described in Appendix A1. In conducting our review, we have identified several opportunities for improvement in the control environment, as identified in Section 04 below.

3.3 Value for Money

Effective management of risk inherently achieves value for money by mitigating the crystallisation of risks that are likely to result in reduced income or additional expenditure. Where organisations have not been able to implement an effective approach to risk management, they become increasing susceptible to threats to business operations; and risk the loss of reputation and finance.

The Risk Management Policy and Corporate Risk Register provides a clear overview of how the ICO manages risks, including an assessment of risks and the mitigating controls.

The ICO is currently using Microsoft Excel spreadsheets to document and monitor risks. Sometimes we see peer organisations use risk management database systems to record risks. Systems often have automated email alerts and reporting facilities which could reduce staff time in administering the risk registers. That said, a formal cost v benefit analysis would need to be undertaken. This is something the ICO may wish to consider, however, we have not raised a recommendation in respect of this matter.

3.4 Sector Comparison

Embedding a risk-based culture across all levels of an organisation may be seen as a large piece of labour-intensive work, however this is not always the case. It is often the awareness that the processes conducted by employees are in fact steps taken to mitigate risk which is the issue. For example, all job roles within the ICO will relate to risk in some way. In the finance department this may be ensuring finances are in line with the

budgets, whereas in the Public Advice and Data Protection department, ensuring complaints are addressed effectively and efficiently is the way in which risks are mitigated. Poor risk management in any department could lead to the ICO not achieving its corporate objectives. The focus for the ICO at present is to ensure the risk management framework aligns to the ICO25 Strategy.

In most cases, employees carry out their roles without thinking about risk, which in fact is the golden thread through all activities undertaken. Therefore, it is management's responsibility to explain the link between the processes undertaken to manage risk and how the team is performing in terms of mitigating the risks facing the organisation. We understand that the ICO are in the process of developing online risk management training that will be delivered to all staff. This will ensure all employees are aware of the importance of risk management, and the role they play.

Currently, the ICO defines its risk appetite via 22 statements, covering key operations and their respective appetite. This is higher than we generally see at peer organisations. The Director of Corporate Affairs & Governance confirmed that this was a conscious choice made by the Management Board, in order to give greater control over differing areas and allow staff to make more sense of how risk management relates to them individually.

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	Directorate Risk Registers The Risk and Governance department created standard templates for directorate business plans, with an accompanying risk register. At the time of the audit, four directorates did not have a completed risk register and or an assigned Risk Champion. These are: Regulatory Futures, Regulatory Assurance, Corporate Communications and People Services. Of the remaining 13 Risk Registers which were complete, we identified the following: • Two Risk Registers in which owners were not assigned to each risk. This was the Finance and Estates Risk Register and the High Priority Investigations (HPI), Insight, Intel & Relationship Management Risk Register; • Six Risk Registers in which each risk did not have scores assigned to each risk (Finance & Estates; Legal Services; HPI, Insight, Intel & Relationship Management; Investigations; Change and Transformation; Economic Analysis) • Four Risk Registers where due dates/action dates were not recorded for each risk (Digital IT & Business Services; Parliamentary Government Affairs (PGA); Finance and Estates; Tech and Innovation); and	The ICO should: 1) Ensure all directorates have a complete risk register in place and an assigned Risk Champion; 2) Remind Directors and Risk Champions of the information required to be completed in the directorate risk registers; and 3) Provide training to Directors/Risk Champions covering the principles of risk scoring and risk treatment.	**Medium**	1) We will ensure all directorates have a completed risk register in place for 2023/24 objectives. Where directorates need further support, we will facilitate risk workshops 2) We will have assigned risk champions for each directorate and remind directors and champions of the information required in the risk registers 3) We have provided training to directors and risk champions on risk scoring and treatment but will provide refresher training as part of risk workshops where appropriate	End of September 2023 End of April 2023 Completed Head of Planning, Risk & Governance / Risk & Business Continuity Manager

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
	• Seven Risk Registers in which there were instances of mitigating actions not reducing, or sometimes, increasing the net risk score. This indicates the controls are not effective mitigation or the risks have not been correctly scored (Digital IT & Business Services; PGA; Finance and Estates; Technology & Innovation; Freedom of Information; Economic Analysis; Change & Transformation). *Risk: Directorate risks are not captured, scrutinised or discussed. Risk scores are absent or incorrect, affecting the ICO's decision making processes in response to directorate risks.*				
4.2	**ICO25 Strategy Alignment** Risk registers should link risks to aims and objectives to help ensure risks remain focused on what the organisation is trying to achieve. The alignment of risk management to strategic objectives is vital if the process is to be effective at managing strategic risks. Due to the timing of this audit, risk management policies and procedures and directorate business plans had not yet been updated to reflect the new ICO25 strategy, implemented in November 2022. The Risk and Governance Department are in the process of updating documentation to reflect this. In addition, the ICO's Intelligence Team conduct an annual Strategic Threat Assessment which is used to inform horizon scanning in relation to risk management, covering the regulatory priorities. This exercise was last completed in October 2021 and therefore is overdue, however, we understand that this is due to the implementation of the ICO25 Strategy.	As planned, the ICO should review and update the Risk Management framework to reflect the new ICO25 Strategy, ensuring clear links between corporate risks and aims. This should include directorate business plans and Risk Registers.	**Medium**	The corporate risk register is currently under review and the directorate business plans and risk register templates provide for clear linkage to the ICO25 strategy.	End of April 2023 Head of Planning, Risk & Governance / Risk & Business Continuity Manager

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
	The Risk Management Policy was reviewed and approved by the Audit and Risk Committee in January 2023, following conclusion of fieldwork. *Risk: Risks to achievement of strategic priorities may not be identified where not explicitly stated on the strategic risk register. Reduced understanding of which strategic priorities may not be achieved, should a risk materialise.*				
4.3	**Risk Maturity Assessment** The ICO's last risk maturity assessment was completed in June 2019, when a questionnaire was sent to managers at Director and Head of Department level. The questions related to risk processes to give an indication of the ICO's risk maturity, and additionally asked about risk culture. There were no plans for a periodic reassessment of risk maturity, however, we were informed that this will be refreshed following implementation of ICO 25 strategy. *Risk: The ICO is unaware of the effectiveness of its risk management processes due to a lack of a risk maturity assessment.*	As planned, the ICO should re-assess its risk maturity and complete periodic reassessments.	**Low**	Risk maturity will be reassessed and reported to the October ARC meeting.	October 2023 Head of Planning, Risk & Governance / Risk & Business Continuity Manager
4.4	**Risk Appetite Statements** The ICO has 22 defined risk appetite statements in place across its activities. We compared these to the risk appetite statements contained within the CRR and identified two areas (organisational controls and compliance and regulatory investigation) in which the defined appetite recorded differed. The Risk & Business Continuity Manager confirmed that this was an oversight due to resourcing issues and needed to be updated.	The ICO should review the risk appetite statements within the Corporate Risk Register and ensure these align to the Risk Management Policy.	**Low**	The risk appetite statements are currently being reviewed and once approved by Management Board the corporate risk register will be updated as required	End of June 2023 Head of Planning, Risk & Governance / Risk & Business Continuity Manager

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
	Risk: Risk owners are unaware of risk appetite, leading to incorrect assessment of risk and poor decisions being made.				
4.5	**Risk Management Policy** We identified some areas of good practice that we see included in peers' policies that are not currently included in the ICO's Risk Management Policy or Procedure. These are: • Top-down endorsement of the importance of risk management from senior staff members (e.g. the Commissioner); • Explicit reference to directorate risk registers, so staff are aware these risk registers follow the same risk management processes; and • The importance of ensuring inherent risk scores reduce to be residual risk scores. *Risk: Staff are unaware of the correct actions to take as these are not reflected in the Risk Management Policy*	The ICO should consider including the points highlighted within the observation in the Risk Management Policy and Procedure.	**Low**	We will consider including the top down endorsement as a foreword to the policy. More explicit reference to the directorate risk registers will be incorporated into the risk procedure We will include further clarity in the risk management procedure of how inherent (gross) and residual (net) risk scores inter-relate	End of Feb 2024 End of April 2023 End of April 2023 Head of Planning, Risk & Governance / Risk & Business Continuity Manager
4.6	**Risk Management and Internal Controls Goals** The Risk Management Policy sets out four risk management and internal control goals, supported by actions. For example, Goal 3 which is to 'ensure that staff have the skills and knowledge they need to fulfil their risk management responsibilities' includes an action to provide training, guidance and templates. These actions are not currently monitored or reported on formally. *Risk: Lack of ongoing monitoring and oversight of the Risk Management and Internal Controls Goals means progress is not recorded and the goals not achieved.*	The ICO should consider formally monitoring progress against its risk management and internal controls goals.	**Low**	Agreed. An action plan will be produced and reported against to RGB	End of April 2023 Head of Planning, Risk & Governance / Risk & Business Continuity Manager

A1 Audit Information

Audit Control Schedule	
Client contacts:	Louise Byers, Director of Corporate Planning, Risk Governance Joanne Butler, Head of Planning, Risk & Governance Chris Braithwaite, Senior Corporate Governance Manager Caroline Robinson, Risk and Business Continuity Manager Claire Churchill, Corporate Gov and Secretariat Group manager Fiona Wilcock, Corporate Governance Officer
Internal Audit Team:	Peter Cudlip, Partner Hannah Parker, Manager Jessica Holt, Assistant Manager
Finish on site/ Exit meeting:	9 January 2023
Last information received:	12 January 2023
Draft report issued:	15 February 2023
Management responses received:	16 February 2023
Final report issued:	17 February 2023

Scope and Objectives

Audit objective: To evaluate and assess the adequacy and effectiveness of the ICO's arrangements for the risk management framework and processes.

- **Framework** – There is no overarching risk management framework in place. The framework does not align to the ICO's strategy.
- **Risk maturity assessment** –An assessment of the ICO's risk maturity has not been undertaken or is not reviewed and updated regularly.
- **Risk appetite -** Risk appetite statements are not in place, or not reviewed and endorsed by senior management and the Board.
- **Risk registers**– Adequate and appropriate risk registers are not in place. Risks are not captured, moderated or discussed.
- **Risk management awareness –** Staff are unaware of their roles and responsibilities for the management of risk across the organisation.
- **Risk registers –** Adequate and appropriate risk registers are not in place. Risks are not captured, scrutinised or discussed. Risk registers s are not moderated. Untimely escalation of risks for consideration by key officers, resulting in inadequate resourcing to mitigate risks and poor decision making.
- **Risk scoring-** Scoring of risks does not clearly identify how risks are scored pre- and post-mitigation. Scoring of risk across the organisation is inconsistent leading to ineffective scrutiny of risks.
- **Mitigating actions-** Lack of ownership of mitigating actions, leading to untimely mitigating controls or prolonged exposure to risks which may materialise.
- **Monitoring and reporting-** Insufficient scrutiny and oversight of key risks and risk management and assurance arrangements, resulting in poor decision making about allocation of resources to appropriately mitigate risk.
- **Horizon scanning** - Horizon scanning is not undertaken, leaving the ICO inadequately prepared for future changes or threats

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
Manager, 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