



Information Commissioner's Office

Internal Audit Report: Performance Management & Management Information

May 2022

mazars

Contents

01 Introduction	1
02 Background	1
03 Key Findings	2
3.1 Examples of areas where controls are operating reliably	2
3.2 Risk Management	2
3.3 Value for Money	3
3.4 Sector Comparison	3
04 Areas for Further Improvement and Action Plan	5
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 2021/22, we have undertaken a review of the Information Commissioner's Office (ICO) arrangements for performance management and reporting of management information. We have reviewed key controls to assess whether the ICO's framework and processes are designed and operating effectively.

Our review assessed the following risk areas:

- Performance Management Framework;
- Strategic Alignment;
- Key Performance Indicators (KPIs);
- Information Quality
- Performance Management Monitoring; and,
- Reporting.

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

We are grateful to the Head of Planning, Risk and Governance, the Group Managers Planning and Performance, and Heads of Service who were interviewed, for their assistance throughout the audit fieldwork.

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

Performance management is a key operational area for any organisation, as it enables the assessment and continuous improvement of business processes and performance across operational functions. It is imperative that organisations have adequate controls in place for performance management to drive improvement and ensure achievement of their strategic and operational objectives.

The ICO's Information Rights Strategic Plan 2017-21 (IRSP) sets out the ICO's mission, vision and six strategic goals. The IRSP supports the statutory responsibilities of the Information Commissioner, with performance against the IRSP strategic goals reported annually in the Annual Report and Accounts which are laid before Parliament each summer. The 2017-21 IRSP plan has been extended to July 2022, giving opportunity for the new Information Commissioner to set out a subsequent ICO Plan with a new vision and strategic objectives.


Underlying the IRSP and to support the achievement of the strategic goals, the ICO has established an annual planning and budgeting process. The process involves the development and refresh of Directorate Business Plans, including budgeting for projects and business as usual. The Business Plans also set out how performance is set to be monitored against objectives and recording of performance measures informing scorecards to be presented at quarterly 'Challenge and Review Sessions'.

The Planning and Performance Team are responsible for overseeing the planning and performance process; ensuring that the process is in place and delivers meaningful and robust plans and working with Finance to ensure there are budgets which support the achievement of ICO strategic goals; and that performance is monitored and feeds into changes to plans and budgets as necessary.

When organisations set out their business strategies it is important that performance indicators are set so that those charged with governance can effectively monitor whether objectives are being met. Against these KPIs, achievable yet challenging targets should be set to drive improved performance and continuous development.

As part of the ICO's annual budget and business planning process, Directorate Business Plans are put together setting out key objectives for the forthcoming year, which should include a performance measure or target. In the 2021-22 financial year, the ICO have developed quarterly 'challenge' sessions whereby Directors present their performance scorecards to receive (and give) challenge, feedback and support to their peers. The sessions also inform the corporate performance scorecard and reporting to Management Board as a means of providing cross-office opportunity to share potentially impactful management information.

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>Overall, 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
-	2	-	2

3.1 Examples of areas where controls are operating reliably

- The ICO's Information Right's Strategic Plan (IRSP) sets out the Information Commissioner's mission, vision and six strategic goals. The IRSP supports the statutory responsibilities as well as outlining sub-priorities to the six strategic goals.
- The ICO's performance management framework is updated annually as part of the Business Planning process. The Business Planning Team have developed guidance documents which are made available to all key stakeholders. Our review confirmed that guidance is published on the ICO's staff intranet, ICON, for staff reference.

Directorate Business Plans are refreshed every year, with template plans updated and shared with Heads of Service to ensure that performance measures and targets are captured in the development of objectives for the forthcoming year.

Our review confirmed that the Business Plan template for the 2021-22 year included a 'Performance Scorecard' tab, aiming to capture performance updates for each of the key objectives set for the respective Directorate. The template includes frequency of reporting, target and responsible officer, as well as any linked corporate strategies and risks, ensuring an element of strategic alignment.

- The ICO's performance management information and data is recorded and collated through various means depending on the Directorate. Many of the ICO's services are unique in that performance cannot be easily quantified due to the qualitative nature, such as Legal, Regulatory and Policy services. However, Directorates such as Investigations, Data Protection Compliance and Digital IT and Business Services rely on management systems such as ICE and Crimson to record and report performance.

Our review sample tested three Directorates KPIs and management information reported at the latest management Quarterly Challenge session (Q3) and confirmed the accuracy of all three Directorate's KPIs being traced back to ICE or Crimson raw data.

3.2 Risk Management

Risk management and performance management are closely aligned to one another. The ICO's business planning process and development of Business Plans requires each Directorate to ensure that where appropriate, key objectives are traceable to Corporate Risks as recorded in the Corporate Risk Register.

Our review sample tested 10 complete Business Plans for the 2021-22 financial year. Of the 10 tested, we identified that only five (50%) of the Business Plans had appropriately traced key objectives to the Corporate Risk Register, referencing the risk associated. We have therefore raised a recommendation in respect of this issue, along with the ICO considering the below observation. Please see **Section 04** for more details of the recommendation raised.

From our experience, other organisations capture both risk management and performance management well, through the use of Strategic Risk Maps. Strategic Risk Maps intend to define an organisations approach to mitigating risks and maximising opportunities aligned to business activities and thus supporting the achievement of strategic objectives. Where underperformance is identified, organisations use the Strategic Risk Map to ensure action is taken to mitigate the underlying risk associated with poor performance. Thus, the risk of not performing and/or achieving against the objectives will be reduced and captured.

3.3 Value for Money

Value for money (VFM) implications arise in respect of performance management and reporting of management information not only in terms of KPIs, which in themselves identify VFM specific matters, but also how they enable the organisation to identify its current performance and respond, ensuring limited resources are put to best use and to maximise the ability to achieve its objectives.

Implications also arise from the extent of underlying processes and systems by which KPIs and management information can be identified, collated, monitored and reported on to senior managers.

In relation to system processes for performance management and management information, the ICO currently operate a mixture of system and manual records; however, spreadsheets are used in the main. For instance, our review identified that the ICO use spreadsheets for developing Business Plans and quarterly reporting at Challenge sessions. We understand that using automated methods for collecting data is not always practical or realistic, particularly in respect to some of the ICO's Policy or Legal services, however, given the investment that would be required, the ICO may wish to consider a cost versus benefit analysis to support longer-term achievement of VFM through process efficiency. We have raised a recommendation in relation to this in **Section 04**.

3.4 Sector Comparison

Reporting Methodologies

Typically, we see that organisations that manage performance well, have developed an overarching document that sets out the methodologies for compiling performance reports. These documents or strategies outline

proposed performance frameworks, including clear and comprehensive calculation methodologies, roles and responsibilities for reporting, data sources, rationale for allocations of weightings and RAG banding, and any required data validation processes.

The ICO currently have three overarching documents setting out the Business Planning process, ultimately informing the performance framework. These guidance documents set out the general processes for developing Business Plans, performance measures and the expectation of quarterly Challenge and Review sessions. However, our review of the guidance available as well as the IRSP, identified that the ICO do not clearly outline the reporting methodologies, frequency, nor roles and responsibilities for reporting performance outside the quarterly challenge sessions and Management Board meetings. It is not clear how Directorates should review operational and sub-Board management information. We have therefore raised a recommendation in relation to this. Please see **Section 04, 4.1** for more details.

Weighted Scoring Model

In addition to reporting methodologies, we also see those organisations who manage performance well use weighted scoring models. The use of a weighted scoring model allows organisations to prioritise and contextualise performance scores for each KPI (within reason). Often these are allocated on a fairly arbitrary basis, however, the weighting allows specific indicators to emphasise where under/ over performance may affect the achievement of strategic objectives.

Typically, weighted scoring models are reviewed by either Board or sub-Board committees annually, with subsequent revisions made to the performance framework/ methodology that sets out how weightings are to be allocated.

Whilst weighted scoring models may not be suitable for all Directorates across the ICO, management may wish to consider utilising such models when reviewing the performance framework to determine which performance indicators are to be reported at an operational level and which should be focussed at strategic level. Equally, the ICO could use a weighted approach when considering impact reporting. Please see **recommendations 4.3 and 4.2** respectively for more details.

Impact Assessment

One of the areas that organisations struggle to capture, including the ICO, is the real-life impact of their work on key stakeholders. Where we have seen organisations do this well, impact has been a core metric when establishing performance indicators.

In order to ensure this process is effective and impact is appropriately captured, some organisations have developed an impact model or strategy. An Impact Model, in this instance, is a high-level summary of how an organisation expects staff to consider impact in the delivery of day-to-day business to achieve strategic goals or priorities (including projects).

Best practice includes the development of supporting user guides which sets out how staff should plan in an impact-focused way, setting out the high level aims and intermediate changes the work should achieve, and then how to evaluate whether or not the work has progressed or achieved them in the 'real-world'.

We have also seen organisations develop 'Impact Forums' which are set up to ensure that all staff understand and can demonstrate impact both for external stakeholders, as well as making sure they are doing the right things to create change. Impact models and strategies include action plans to outline how organisations can improve their understanding of "what works" to make more informed decisions about what interventions to make in driving forward strategic goals.

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>Performance Management Framework</p> <p><i>Observation:</i> We noted a number of issues with the design and operation of the ICO's performance management framework.</p> <p>We have categorised these as follows:</p> <p>Identification of strategic performance</p> <p>The ICO's strategic direction and goals are driven by the Information Rights Strategic Plan (IRSP) 2017-21.</p> <p>Our review of the IRSP confirmed that the ICO's six strategic goals are underpinned by strategic priorities, however, these do not clearly outline specific targets, outcomes or performance measures that can be used to determine progress or performance against each priority. Nor are persons responsible outlined to ensure accountability against these objectives.</p> <p>Identification of operational performance</p> <p>The ICO's approach to operational performance is to develop annual Directorate Business Plans that align to the IRSP. From a sample of 10 Directorate Business Plans (18 in total) five had not appropriately included any performance indicators, nor reference to corporate risks (where appropriate), strategic goals or priorities.</p> <p>Additionally, our review of the ICO's Business Planning guidance identified that the ICO do not clearly outline the reporting methodologies, frequency, or roles and</p>	<p><i>As the ICO are in a period of transition with the development of the new ICO Plan which will supersede the current IRSP, this recommendation focuses on actions to consider with respect to the new Plan.</i></p> <p>The ICO should ensure that a top-down or "golden thread" approach is taken to performance, to include the following: -</p> <ul style="list-style-type: none"> • Goals and priorities are clear and specific in the outcome they set out to achieve, • Measurable targets and indicators are developed to clearly demonstrate achievement of goals, • Persons responsible and reporting-lines are assigned for accountability, and • Where operational or Business Plan sub-objectives are 	2	<p>These recommendations build on the work already been undertaken to address the areas identified.</p> <p>The new ICO Plan is already being developed and incorporates performance measures to ensure there are clear targets and indicators to measure success.</p> <p>Work to capture impact and sentiment measures is already underway as part of our Management Board Scorecard development (as evidenced on our website). These are going to consider how our work impacts individuals, business and organisations we provide services to, as well as the wider impacts of our work on the digital economy and services.</p> <p>Our quarterly corporate 'Challenge and Review' sessions ensure there is a clear process for discussing, reviewing and challenging performance. We also plan to develop Executive Directorate level scorecards,</p>	<p>31 March 2023</p> <p>Jo Butler – Head of Planning, Risk and Governance</p>

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
	<p>responsibilities for reporting operational performance. However, we confirmed that the Technology and Innovation Directorate have established a Technology and Innovation Board, who review performance on a monthly basis, yet other directorates review data and management information informally through team meetings without recording actions.</p> <p>Identification and capture of impact</p> <p>Through review of Business Plans, we identified that the ICO do not effectively capture and measure the impact of outcomes and performance on the general public and key stakeholders. Management confirmed that the current performance process favours quantitative measures, with qualitative services such as Legal, Regulatory or Policy struggling to effectively quantify how to measure performance based on subjective outcomes, and thus do not capture the impact of delivery.</p> <p><i>Risk: The ICO's performance management framework is not fit-for-purpose and does not appropriately capture performance against the strategic goals and priorities as set out in the overarching IRSP.</i></p>	<p>developed, these are clearly aligned and traceable to strategic goals and priorities, outlining monitoring arrangements.</p> <ul style="list-style-type: none"> • Capture of real-world impact of outcomes and performance, in the delivery of services to the general public and key stakeholders. 		<p>building on the measures in the business plans, to ensure this process is replicated at Directorate level.</p> <p>All Business Plans for 2022/23 have now been reviewed and published to staff. Links to the new ICO Plan goals will be integrated into our templates, process and guidance for Business Planning 2023/24.</p> <p>The ICO Plan is currently scheduled for consultation in the summer of 2022, and we therefore anticipate being able to deliver the ensuing aspects of the recommendation by the end of the financial year; 31 March 2023.</p> <p>Although we have begun work to capture the real-world impact of our regulatory work this is a longer-term research ambition which we will ensure we achieve through focusing on an action plan identifying how best we can measure impact and outcomes.</p>	
4.2	<p>Performance Reporting Roles and Responsibilities</p> <p><i>Observation:</i> In the 2021-22 financial year, the ICO developed quarterly 'Challenge and Review' sessions where Directors present their performance scorecards to receive, challenge, feedback and support from their peers. The sessions also inform the corporate</p>	<p>The ICO should review the current performance framework's reporting-lines to ensure that KPIs and management information are</p>	2	<p>The development of the corporate scorecard, and its publication, is a significant step forward in ensuring there is a mechanism to report performance on a regular basis to Management Board (of which all ET are members) and to</p>	<p>31 March 2023</p> <p>Jo Butler – Head of Planning, Risk and Governance</p>

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
	<p>performance scorecard and reporting to Management Board as a means of providing cross-office opportunity to share potentially impactful management information.</p> <p>However, we identified that the Challenge and Review sessions report by exception, on the more significant performance measures, or those that may impact other Directorates.</p> <p>Additionally, not all Directors attend the Challenge and Review sessions, and the ICO do not have any formal reporting of performance at Executive Team (ET) or Senior Leadership Team (SLT) meetings.</p> <p><i>Risk: Performance reports and KPIs are not appropriately or effectively delegated across the ICO's senior management teams.</i></p>	<p>appropriately delivered and delegated across strategic and operational levels. KPIs reported by exception at quarterly Challenge and Review Sessions is effective, providing all other KPIs are reviewed operationally.</p> <p>The ICO should also ensure that monitoring mechanisms at operational level are consistent, with any corrective actions recorded and monitored.</p>		<p>our stakeholders (as it is published on our website.)</p> <p>The quarterly corporate challenge and review sessions are attended by all Directors, where they are available. This is therefore all of SLT. As part of this, all business plans and performance updates are made available to Directors.</p> <p>We will continue to review the current performance framework's reporting lines, to dovetail reporting requirements for our new Plan. Our review will ensure monitoring mechanisms at operational level are part of a consistent review process, enhancing the existing reporting by exception, and the process will be agreed with the Executive Team.</p> <p>We will also develop Executive Director level scorecards to ensure that all relevant KPIs are reported on regularly.</p> <p>In order to demonstrate evidence of delivery, one fully completed calendar quarter of reporting will need to follow the launch of our new Plan, and therefore the end of the financial year is proposed as a timeline for implementation.</p>	

Ref	Observation/Risk	Recommendation	Priority	Management response	Timescale/ responsibility
4.3	<p>System Automation</p> <p>In relation to system processes for performance management and management information, the ICO currently operate a mixture of system and manual records; however, spreadsheets are used in the main. For instance, our review identified that the ICO use spreadsheets for developing Business Plans and quarterly reporting at Challenge sessions. We understand that using automated methods for collecting data is not always practical or realistic, particularly in respect to some of the ICO's Policy or Legal services, however, given the investment that would be required, the ICO may wish to consider a cost versus benefit analysis to support longer-term achievement of VFM through process efficiency.</p>	<p>The ICO should consider a cost versus benefit analysis for the automation of systems for performance management and management information</p>	3	<p>The ICO will undertake a cost versus benefit analysis for the automation of systems and align this with consideration of our wider future ambitions around data visualisation (e.g., using MS Power BI) to unify data presentation.</p>	<p>31 December 2022</p> <p>Jo Butler – Head of Planning, Risk and Governance</p>

A1 Audit Information

Audit Control Schedule	
Client contacts:	Louise Byers – Director of Risk and Governance Joanne Butler – Head of Risk and Governance Rob Barnett – Planning and Performance Group Manager
Internal Audit Team:	Peter Cudlip, Partner Darren Jones, Manager Chris Hogan, Senior Auditor
Finish on site/ Exit meeting:	01 March 2022
Last information received:	15 March 2022
Draft report issued:	20 April 2022
Management responses received:	12 May 2022
Final report issued:	18 May 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 Performance Reporting and Information Management. Our review considered the following risks:

- Performance Management Framework** – There is no performance management framework in place which shows agreed timescales, responsibilities and targets to be achieved.
In addition, the framework doesn’t specify how and when performance should be reported and to whom this should be reported to.
- Strategic Alignment** – The ICOs performance management framework and KPIs do not align with the objectives set within the Information Rights Strategic Plan, nor the service standards outlined in the ICO’s Service Charter.
- Key Performance Indicators** – KPIs are not sufficiently challenging, leading to a potential reduction in real world impacts being provided.
KPIs set do not have a direct link to the aims and objectives of the ICO, and the methodology for calculating KPIs is not appropriate.
- Information Quality** – Poor data quality results in inaccurate performance information and subsequently poor strategic and operational decisions being made.
- Performance Management Monitoring** - Performance is not reported on a timely basis to the appropriate level of management, resulting in issues not being identified and rectified on a timely basis.
Performance is not reviewed on a regular basis, in-line with the performance management framework.
- Reporting** – Performance reporting isn’t used to identify and drive improvements, leading to failure to correct/ identify operation issues.
Performance reports are not delivered to those with the ability to implement solutions, for example the audit committee.

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, 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