Audit and Risk Committee Annual Report 2022/23

Introduction

The Information Commissioner's Audit and Risk Committee (the Committee) provides scrutiny, oversight and assurance of risk control and governance procedures. Minutes of its meetings are available on the ICO's website at www.ico.org.uk.

This report was agreed at the Committee's meeting on 30 June 2023. It covers the work of the Audit and Risk Committee during the period April 2022 to March 2023, with additional detail about reports received in April 2023 and June 2023 relating to work completed in respect of the year 2022/23.

Summary

The Audit and Risk Committee recognises that there has been significant progress across its remit during the year. Committee members have been provided with timely and comprehensive information on the ICO's control environment, financial position, risk profile and governance arrangements, and have used their knowledge and experience to ask rigorous questions of management throughout the year.

Internal and external auditors have provided independent assurance to the Committee. The Committee are pleased that the internal auditors' opinion of 'substantial' reflects an effective framework of governance, risk management, and controls, as well as the Committee's focus on timely implementation of internal audit recommendations.

Membership and attendance

The Committee's chair is Ailsa Beaton, who is a non-executive director and member of the Management Board.

There are two other members of the Audit and Risk Committee:

- an independent member - Jayne Scott; and
- a non-executive director who is also a member of the Management Board – Jane McCall until 3 October 2022, and Ranil Boteju from 3 October 2022.

In 2022/23, the Committee met on 25 April 2022, 20 June 2022, 10 October 2022 and 17 January 2023. Attendance of members at Committee meetings is detailed in the ICO's Annual Report and Accounts 2022/23. All meetings were held virtually. Secretariat for the meetings was provided by the Corporate Governance Team.

Representatives of external audit and internal audit attended all of the meetings and meet confidentially with the Committee members prior to each meeting. The ICO's external audit function in 2022/23 was provided by the National Audit Office, with Deloitte working on their behalf.

The ICO's internal audit function was provided by Mazars up to 31 March 2023. Representatives of Mazars attended the meetings up to April 2023. From 1 April 2023, the ICO's internal audit function was provided by the Government Internal Audit Agency (GIAA). Representatives of GIAA attended the meetings from January 2023 onwards.

Meetings during 2022/23

The Committee considers the following issues as standing items at all of its meetings:

- an update on current ICO issues from the Deputy Chief Executive Officer;
- updates to the corporate risk register;
- the most recent monthly income and expenditure report;
- progress reports from the internal and external auditors;
- discussion of audit reports and progress in completing recommendations from internal and external audits;
- reports on any single-tender contract awards over £25k; and
- updates on whether there have been any reported whistleblowing, fraud or security incidents, and details of these where appropriate.

In addition, during the year the Committee considered the following matters:

- the Annual Report & Accounts for 2021/22 were considered during the year, and the Annual Report & Accounts for 2022/23 have been considered at subsequent meetings in April 2023 and June 2023;
- lessons learned from the production of the 2021/22 annual report;
- approach to the production of the 2022/23 annual report, a summary of any changes to accounting standards, and a summary of specialist reports to be commissioned from third parties on areas of particular judgements, estimates or valuations.

- the Arms-Length Bodies' Audit Committee Chairs' Assurance Letter to the Department for Culture, Media and Sport (DCMS) for 2021/22 was considered during the year, and the Arms-Length Bodies' Audit Committee Chairs' Assurance Letter to the Department for Science, Innovation and Technology (DSIT) for 2022/23 was considered at a subsequent meeting in June 2023;
- the NAO's Audit and Risk Assurance Committee effectiveness tool;
- internal audit plan for 2021/22, as well as proposals for internal audit provision from April 2023, and an indicative three-year internal audit plan;
- an update on the ICO's approach to risk management, an annual review of the full risk register and an annual review of the Risk Management Policy and Risk Appetite Statement;
- information on business continuity, including the annual update to the strategy statement;
- deep dives into the arrangements that are in place to ensure the ICO's compliance with all legislative requirements, and assurance on the ICO's compliance with Government functional standards;
- assurance on: the ICO's cyber security arrangements including a ransomware desktop assessment; procurement; the ICO's management of issues relating to estates, climate and environment; the ICO's compliance with its own Accountability Framework; its compliance with Data Protection legislation; and its compliance with the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018; and
- the ICO's Reserves Policy.

Plans during 2023/24

During 2023/24, as well as continuing to receive further iterations of the reports set out above, the Committee will focus on:

- Continued oversight of the delivery of the internal and external audit plans.
- Ongoing monitoring of the financial position of the organisation, including reviewing the annual report and financial statements.
- Oversight of the management of risk, including the mitigating actions and controls in place to manage significant risks to the organisation, including a review of our Risk Management Policy.

- Identifying areas for additional assurance to ensure the Committee can provide an opinion at year end regarding the ICO's control environment.
- Continued monitoring of the risk landscape and assessing implications to the ICO as we build on our organisation-wide resilience and continue to improve our risk management framework. This will also include a review of our Business Continuity Strategy Statement.

The Audit and Risk Committee will also keep abreast of the ICO25 strategic plan and any strategic change and transformation priorities as they develop in the coming months and years, and the impact that any of these changes may have on future audits and overall assurance.

Internal and external audit

The Committee reviewed the internal audit plan and progress against it on a continual basis. During the year, the Committee considered internal audit reviews by Mazars of:

- workforce planning (from the 2021/22 internal audit programme);
- performance reporting and management information (from the 2021/22 internal audit programme); and
- core financial controls – corporate charge cards.

At its subsequent meeting in April 2023, the Committee considered internal audit reviews by Mazars of:

- case management;
- risk management;
- procurement and contract management;
- guidance development; and
- civil monetary penalty recording.

Mazars made 32 formal recommendations in the six areas audited during 2022/23. There were also 26 audit recommendations from audits in 2021/22 which had not been due for completion before the end of that year.

A summary of the due dates of the 58 recommendations is shown in the following table: 25 recommendations were due for implementation by 31 March 2023, and 33 recommendations were not due for implementation until after the year end.

Mazars published an interim review in July 2022, considering the ongoing Cyber Security recommendations, and confirmed that five had been implemented.

Mazars published a year end review in April 2023, considering the remaining 20 recommendations which had been due for implementation by 31 March 2023, as well as three recommendations which had not been due for completion by this date but that the ICO considered complete. Of these 23 recommendations, Mazars confirmed that 22 had been implemented (96%) and one was proposed to be closed (4%). In addition Mazars made three new recommendations in relation to Cyber Security.

33 recommendations will be considered in the next follow up review, at the end of 2023/24.

	Total	**Due by 31/3/23**	**Due after 31/3/23**
Open recommendations	58	25	33
Confirmed as complete during July 22 follow up	(5)	(5)	-
Confirmed as compete during March 23 follow up	(23)	(20)	(3)
New recommendations raised during March 23 follow up	3	-	3
Remaining recommendations	**33**	**-**	**33**

Mazars' Annual Internal Audit Report 2022/23 concluded that: "On the basis of our audit work, our opinion on the framework of governance, risk management, and control is 'substantial' in its overall adequacy and effectiveness. Certain weaknesses and exceptions were highlighted by our audit work. No 'high' priority findings have been raised, however, limited assurance was provided in respect of Corporate Charge Card processes. These matters have been discussed with management, to whom we have made several recommendations. All of these have been, or are in the process of being addressed, as detailed in our individual reports. An internal audit of Risk Management was completed in the year with a substantial assurance opinion given. The ICO has continued to perform

well with the implementation of recommendations, with 100% of recommendations closed."

"Substantial" is the highest of the four ratings offered by Mazars (who provide annual report opinions of "substantial", "moderate", "limited" and "unsatisfactory"). "Substantial" is defined as "the framework of governance, risk management and control is generally adequate and effective".

The National Audit Office Audit Completion Report 2022/23 concluded that "We anticipate recommending to the Comptroller and Auditor General (C&AG) that he should certify the 2022-23 financial statements with an unqualified audit opinion, without modification in respect of both regularity and the true and fair view."

Audit and Risk Committee opinion

Given the opinion of the internal auditors and external auditors as expressed in their annual reports, and the other information available to it from its work during the year, the Audit and Risk Committee can therefore provide the Commissioner, as Accounting Officer, with reasonable assurance that the ICO's control mechanisms are working satisfactorily.

The Committee is satisfied with the quality of internal and external audit. The Committee believes that, by virtue of this work, it is able to take a measured and diligent view of the quality of financial and other systems of reporting and control within the ICO.

The Committee welcomed the ratings of substantial assurance in: the risk management audit; the guidance development audit; and the civil monetary penalty recording audit. The Committee also welcomed the helpful recommendations in: the case management audit; the performance management and management information audit; the workforce planning audit; and the procurement and contract management audit. The Committee welcomed the detailed recommendations from the corporate charge card audit, and is satisfied that the ICO has appropriate systems of internal control, which work well.

In respect of its own performance the Committee considers that it has directed the internal audit function towards areas relevant to the risks facing the ICO. It has constructively challenged management and the internal audit function. It has received a high level of cooperation and support from all concerned. Responses to audit recommendations from management are positive and the Committee is satisfied that

management within the ICO is committed to maintaining an appropriate level of internal control and prudent use of resources.

This opinion feeds into the Commissioner's drafting of the Governance Statement for 2022/23, which was considered by the Audit and Risk Committee at its April 2023 and June 2023 meetings.

30 June 2023.