

# Audit and Risk Committee Annual Report 2021/22

## 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](http://www.ico.org.uk).

## 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. One is Jane McCall, who is a non-executive director and member of the Management Board. The second is an independent member. Until 31 July 2021, this was Roger Barlow. Roger completed his term as independent member on this date, having spent nine years in this role. Jayne Scott joined the Committee as independent member on 1 August 2021.

The Committee would like to take this opportunity to thank Roger for his outstanding work and contribution to the Audit and Risk Committee during his nine years as independent member.

In 2021/22, the Committee met on 21 June 2021, 18 October 2021, 10 January 2022, 25 February 2022, 25 April 2022 and 20 June 2022. This report was agreed at the Committee's meeting on 20 June 2022.

Attendance of members at Committee meetings is detailed in the ICO's Annual Report and Accounts 2021/22. All meetings were held virtually.

The ICO's external audit function in 2021/22 was provided by the National Audit Office, with Deloitte working on their behalf. The ICO's internal audit function in 2021/22 was provided by Mazars. Representatives of external audit and internal audit attended all of the meetings.

Secretariat for the meetings was provided by the Corporate Governance Team.

## Meetings during 2021/22

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

- A review of the corporate risk register
- The most recent monthly finance 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 2020/21 and for 2021/22, including specific considerations on the treatment of depreciation and ensuring transparency of the collection and remittance of financial penalties in relation to the ICO's regulatory work.
- Lessons learned from the production of the 2020/21 annual report.
- The Arms-Length Bodies' Audit Committee Chairs' Assurance Letter to DCMS for 2020/21 and 2021/22.
- 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.
- The NAO's Good Practice Guidance: Principles of Effective Regulation and its links to DCMS's "Data: a new direction" consultation on the future of data protection; and the NAO's Audit and Risk Committee effectiveness tool.
- Updates on plans for future internal audit provision.
- An update on the ICO's approach to risk management, and an annual review of the full risk register and annual review of the Risk Management Policy. In addition, the Management Board conducted a full review and update to the ICO's Risk Appetite Statement, which is included in that policy.
- Information on business continuity, including the annual update to the strategy statement and specific assurance on preparedness for potential ransomware attacks.
- An overview of the ICO's corporate governance structure.
- Assurance on: the ICO's cyber security arrangements; the ICO's management of issues relating to estates, climate and environment;

the ICO's compliance with its own Accountability Framework; and its compliance with the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018.

## Plans during 2022/23

During 2022/23, 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

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

- Core financial controls
- Cyber security
- Fines recovery
- Performance reporting and management information
- Stakeholder management
- Workforce planning

In these audits, Mazars made 35 formal audit recommendations. There were also nine audit recommendations from audits in 2020/21 which had

not been due for completion during 2020/21. At year end, Mazars reviewed progress with these 44 recommendations and confirmed that all 26 which were due for completion during 2021/22 have been completed. No recommendations were late from their agreed due date. 18 recommendations were not yet due for completion.

Mazars' Annual Internal Audit Report 2021/22 concluded that: "On the basis of our audit work, our opinion on the framework of governance, risk management, and control is Moderate in its overall adequacy and effectiveness. Certain weaknesses and exceptions were highlighted by our audit work and three high priority findings were raised. 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. The ICO's has continued to perform well with the implementation of recommendations, with 100% of recommendations being implemented. In respect of Covid-19, our annual internal audit opinion reflects the revised audit plan agreed and is not limited in scope, to the extent that the assurance provided by internal audit can only ever be reasonable, not absolute."

"Moderate" is the second highest of the four ratings offered by Mazars (who provide annual report opinions of "substantial", "moderate", "limited" and "unsatisfactory"). "Moderate" is defined as "some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control."

The National Audit Office Audit Completion Report 2021/22 concluded that "We anticipate recommending to the Comptroller and Auditor General that he should certify the 2021-22 financial statements of the Information Commissioner's Office with an unqualified audit opinion, without modification in respect of both regularity and the true and fair view on the group financial statements."

### **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 audit for Fines Recovery. The Committee also welcomed the detailed recommendations from the Cyber security audit and is satisfied that the ICO has appropriate systems of internal control, which work well. The Committee also welcomed the helpful recommendations in developing the ICO's Workforce Planning Strategy.

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 2021/22, which was considered by the Audit and Risk Committee at its April 2022 and June 2022 meetings.

20 June 2022.