Audit and Risk Committee annual report 2025/26

Introduction

The Information Commissioner's Office's Audit and Risk Committee ("the Committee") provides scrutiny, oversight and assurance of the ICO's risk control and governance procedures. Minutes of its meetings are available on the ARC page of the ICO's website.

This report was agreed at the Committee's meeting on 18 June 2026. The report covers the Committee's work during the period April 2025 to June 2026.

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:

- an Independent Member - Jayne Scott; and
- a Non-Executive Director who is also a member of the Management Board – David Cooke.

In 2025/26, the Committee met on 24 April 2025, 16 June 2025, 23 October 2025, 20 January 2026 and 26 March 2026. Attendance of members at Committee meetings is detailed in the ICO's Annual Report and Accounts 2025/26. Secretariat for the meetings was provided by the Corporate Governance team.

Representatives of external audit and internal audit attended all of the meetings and met confidentially with the Committee members prior to each meeting.

The ICO's external audit function in 2025/26 was provided by the National Audit Office (NAO) with Deloitte working on their behalf. The ICO's internal audit function in 2025/26 was provided by the Government Internal Audit Agency (GIAA) – the third year of their appointment.

Meetings during 2025/26 and Q1 of 2026/27

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

- update on current ICO issues from the Information Commissioner or Interim Chief Executive Officer Designate;
- updates to the corporate risk register;
- monthly income and expenditure reports;
- 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, insider trading 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 2024/25, and the Annual Report & Accounts for 2025/26 was considered at a subsequent meeting on 18 June 2026;
- lessons learned from the production of the 2024/25 annual report, and implementation progress updates;
- approach to the production of the 2025/26 annual report, including the accounting policies used;
- internal audit performance 2024/25 and 2025/26, audit plans for 2025/26, proposals for the 2026/27 audit plan (which will be approved by the Information Commission) 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, an annual review of the Risk Management Policy and Risk Appetite Statement and a review of Orange Book compliance;
- information on business continuity, including the annual update to the strategy statement;

- deep dives to provide assurance on: compliance with the ICO's statutory obligations; the mitigations and next steps for the AI and automation corporate risk; and the ICO's medium term financial plan;
- assurance on: cyber security arrangements; management of environmental, social and governance (ESG) reporting; the ICO's compliance with its own accountability framework; compliance with Data Protection legislation; and compliance with the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018; and
- a 'light touch' review of the Committee's effectiveness.

Plans during 2026/27

Once governance changes set out in the DUA Act are implemented, the Information Commission will set up its own Audit and Risk Committee, with similar roles and responsibilities to the ICO's Committee. Until then, the current Audit and Risk Committee will continue to perform this function. It is intended that the Committeeis likely to consider the following areas during 2026/27:

- 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 a review of the Risk Management Policy and consideration of the mitigating actions and controls in place to manage significant risks;
- monitoring of the risk landscape and a review of the Business Continuity Strategy Statement.
- identifying any areas for additional assurance, to ensure the Committee can provide an opinion at year end regarding the organisation's control environment;
- risk and audit horizon scanning; and
- monitoring the organisation's strategic change and transformation priorities in the short and medium term, and the impact 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 the following internal audit reviews:

- Online accessibility compliance;

- Finance Target Operating Model (TOM);
- Purchase to pay;
- Implementation of the Enterprise Data Strategy (EDS);
- Better Regulatory Interventions (BRI) governance;
- Guidance development;
- People survey action planning and implementation;
- Data analysis (advisory audit); and
- Payroll (advisory audit).

Internal audit made 18 recommendations from their audits during 2025/26, of which 11 were due for implementation before the year end. The remaining seven recommendations are due for implementation during 2026/27.

Audits undertaken in previous years had also raised 29 recommendations, of which 26 recommendations had a due date during 2025/26 and three recommendations had a due date during 2026/27.

Internal audit follows up on the implementation of recommendations during the year. In total, internal audit reviewed the progress of 38 agreed recommendations which were due during 2025/26 (37 due in 2025/26 and one due in 2026/27). All of these recommendations have been confirmed as closed. This leaves nine recommendations to be addressed during 2026/27.

During the year internal audit identified areas of good practice and opportunities for developing and improving current activities. GIAA's annual audit opinion for 2025/26 stated: *"I am providing an overall Moderate opinion on the framework of governance, risk management and control within the ICO for the year ended 31 March 2026. Based on my assessment, and considering insights from other government bodies we cover, it is my opinion that the Information Commissioner's Office compares favourably in its approach and the maturity of its governance, risk management and control framework."*

Moderate is the second highest of the four ratings offered by GIAA, who provide annual report opinions of substantial, moderate, limited and unsatisfactory. The definition of moderate is: "*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 2025/26 for the external audit concluded that "*We anticipate recommending to the Comptroller and Auditor General (C&AG) that he should certify the 2025/26 financial statements with an unqualified audit opinion,*

without modification in respect of both regularity and the true and fair view on the financial statements."

Audit and Risk Committee opinion

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.

The Committee welcomed the internal auditor's rating of 'substantial assurance' in two areas: online accessibility compliance; and people survey action planning and implementation. The Committee also welcomed the helpful recommendations in seven areas: data analysis; payroll; Finance Target Operating Model (TOM); purchase to pay; implementation of the Enterprise Data Strategy (EDS); Better Regulatory Interventions (BRI) governance; and guidance development.

Given the draft opinion of the internal auditor and verbal reports provided by the external auditor, and the other information available to the Committee from its work during the year, the Audit and Risk Committee can provide Paul Arnold (the ICO's Temporary Acting 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.

This opinion feeds into the Governance Statement for 2025/26, which was also considered by the Audit and Risk Committee at its March 2026 meeting.

18 June 2026.