

## Executive Team – for assurance

**Meeting agenda title:** Update on the work of the Risk and Governance Board

**Meeting date:** 19 January 2023

**Time required:** 10 minutes

**Presenter:** Louise Byers

**Approved by:** Paul Arnold

### 1. Objective

- 1.1. This report provides an update on the work of Risk and Governance Board and gives the Executive Team an opportunity to provide guidance on future work.

The Board continues to focus on its assurance and second line of defence role, with a work programme covering, for example, the ICO's risk and business continuity frameworks and compliance and assurance work.

### 2. Key achievements over the last 6 months

The last update on the work of the Board was provided to ET on 30 June 2022. The report to this meeting identified a number of areas where progress was expected to be achieved in the upcoming 6-12 months. These are included in Annex One for ease of reference.

Progress has been made in all areas identified in the previous report. The key achievements of the Board since June are summarised below, with a reference to the Annex where appropriate.

- 2.1. Oversight of the ICO's risk register, including an annual deep dive review of the risk register in September and oversight of work to revise the register in light of the finalisation of our new corporate strategy, ICO25. The Board has also overseen work to map interdependencies across the risk register, as well reviewing the risks in light of external changes such the economic uncertainty, political changes and the cost of living crisis. This work is regularly reported to the Audit and Risk Committee (ARC) and Management Board. (A6)

- 2.2. Oversight of compliance and assurance processes, including ensuring the effective delivery of internal audit actions and reviewing internal audit reports and challenging management responses to recommendations to ensure they are robust and timescales are realistic but timely. This also includes receiving assurance regarding the arrangements to transition to our new internal audit provider from April 2023 onwards. The Board has also commissioned work to ensure compliance with Government Functional Standards, which is due to be reported back to DCMS in March 2023. (A4) (A5)
- 2.3. Benchmarked the work of the Board through both the DCMS Risk Professionals Network and external review. This has included considering the DCMS risk appetite statement and reviewing a paper on benchmarking with other regulators and information rights bodies both nationally and internationally to ensure our governance and reporting approaches remain aligned with best practice.
- 2.4. Challenging the ICO's cyber security defences and approach, in particularly focussing on gaining assurance over progress on delivering recommendations from Mazar's internal audit and the work with NCSC and Cabinet Office on our cyber defences. This work has been completed in this period. The Board has also received assurance regarding work on ransomware response plans and disaster recovery.
- 2.5. Continued oversight of the Information Risk Governance Group subcommittee, which particularly focuses on the management of the ICO's information risks. This is chaired by Mike Fitzgerald and ensures that our information risks are being identified, mitigated and managed effectively. This subcommittee reports on a six monthly basis to the Risk and Governance Board to provide assurance on the work in this area. (A7)
- 2.6. Review of the ICO's risk policy and risk appetite statement, which will be presented to the March Management Board meeting.
- 2.7. Review of the ICO's business continuity policy and plans, which will be presented to the January ARC meeting.
- 2.8. Lessons learned from the Annual Report production, which has informed the 2022/3 Annual Report timetable and approach, as agreed by ET in December 2022. (A2)

- 2.9. Overseen changes in the governance structures, including the introduction of the People Committee and development of the Regulatory Committee work programme and approach. (A1)
- 2.10. John Kavanagh has joined the Board to give assurance regarding governance transition arrangements, although these have been delayed by the overall delays to the DP Bill. (A3)

### 3. Key challenges over the last 6 months

- 3.1. The key challenge for the Board over the last six months continues to be the work to embed the organisation's risk appetite. Since the last report, extensive work has gone into communicating the risk appetite, using case studies and more accessible language to help teams understand and apply the statements. The Board is aware that the Corporate Governance team have produced a knowledge pack and conducted an internal training programme including tailored case studies, as well as using the ICO's internal communications channels and the newly established Risk Champions network. However, there is more to do to help embed this alongside our prioritisation and decision making approaches as part of the implementation and delivery of ICO25.

### 4. Key areas of activity over the next 6-12 months

- 4.1. Continued oversight of the risk register, including ensuring the register reflects new and emerging risks and opportunities resulting from the implementation of ICO25 and the changing external environment. This will be critical to the success of the delivery of our corporate strategy and is a key priority for the Board in its 'second line of defence' role.
- 4.2. The Board will be critical in ensure the successful transition from our current internal audit provider (Mazars) to our new provider (Government Internal Audit Agency) when our current internal audit contract ends on 31 March 2023. This transition will be supported the Board's work on the 2023/4 internal audit plan, which will be based on a three year plan agreed by ARC in June 2022, with further consultation with relevant Directors and ET.

- 4.3. Reporting on the ICO's compliance with the Government Functional Standards to DCMS, with a requirement to be 'good' in all standards by 31 March 2023.
- 4.4. The delivery of the 2022/3 Annual Report. This is well established process, and ET have already considered and agreed our approach to the next report, however the Board will have oversight of delivery of the timetable and ensure this complex process is delivered on time.
- 4.5. The Board will also make recommendations for the Audit and Risk and Committee and Management Board work programmes for 2022/3.
- 4.6. The Board will receive quarterly updates on the actions identified in our Risk Management and Business Continuity plans to ensure progress in delivering the goals set out in the policies.

## 5. Areas for challenge

- 5.1. Are there any areas of focus that ET would expect to see in the Board's future work which are not covered in this report and any areas that the Board has considered that ET would like further assurance on?

**Author:** Louise Byers

**Consultees:** Corporate Governance Team, Risk and Governance Board.

**List of Annexes:** Annex One - Key Areas of Activity for the next 6-12 months identified in the previous ET report (30 June 2022)

**Publication consideration:** Report can be published internally and externally without redactions.

### **Annex One – Key Areas of Activity for the next 6-12 months identified in the previous ET report (30 June 2022)**

A1. Oversight and assurance over the implementation of new governance structures, for example the People and Regulatory Committees, as well as ensuring that the membership of all Management Board committees is

reviewed in light of the new Committees and any additional NEDs, and their relevant skills and experiences.

A2. Delivery of the Annual Report and Accounts, including undertaking a lessons learnt exercise to identify areas for continuous improvement.

A3. Consideration of any transition arrangements necessary to implement the DP reform proposals, in particular the governance, accountability and reporting requirements a new DP bill may require of the ICO.

A4. Overseeing the move from our current internal auditors to a different provider, as the current internal audit contract ends on 31 March 2023.

A5. Considering and challenging the first outcomes of the compliance and assurance work being undertaken by the Risk and Governance department based on the Government's Functional Standards.

A6. Conducting a deep dive review of the ICO's corporate risk register in advance of the Autumn ARC meeting.

A7. Considering and challenging the first reporting to the Board from the Information Risk Governance Group.