Executive Team – for assurance

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

Meeting date: 17 July 2023

Time required: 20 minutes

Presenter: Louise Byers

Approved by: Louise Byers

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.

1.2. 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

2.1. The last update on the work of the Board was provided to ET on 19 January 2023. 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.

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

a) Continued its oversight of the ICO's risk register, including work to revise the register in line with ICO25 This has included the introduction of four new risks onto the register aligned with ICO25 objectives. These are in relation to research, NIS regulations, prioritisation and transparency. The Board has also reviewed existing risks regarding financial resilience, improving productivity and managing ICO reputation. This work is regularly reported to the Audit and Risk Committee (ARC) and Management Board. (A1)

b) Undertaken a full review of the ICO's risk appetite, including extensive consultation with SLT, ET and Management Board. This work has focussed on three key areas which have been identified as most challenging for our teams relating to people, compliance and our regulatory and legal risk appetites. These new risk appetite statements have been communicated internally through our risk champion network, knowledge packs. The Risk and Governance team as also been working with the Board and wider SLT to identifying examples of the risk appetites in action so we use case studies to demonstrate how the risk appetite can support our teams in their day to day work. The next steps for this work include integrating the risk appetites into our decision making framework. It is worth noting that our risk management work was validated by a substantial assurance internal audit of our risk management processes and policies.

c) Overseen the delivery of the ICO's 2022/3 Annual report including assurance on the timetable as well as reviewing a benchmarking report, identifying areas of good practice from other regulators and data protection authorities which we have incorporated into our report. (A4)

d) Overseen the transition of our internal audit provider from Mazars to the Government Internal Audit Agency. This has been delivered successfully, with an internal audit plan for 2023/4, with input from SLT and ET, agreed by the ARC. This internal audit plan is now being delivered, with Q1 audits on cyber security and conflicts of interest underway. (A2)

e) Reviewed and recommended work programmes for Management Board and ARC. (A5)

f) Undertaken work in relation to compliance, including reviewing the ICO's three lines of defence for the full range of our compliance requirements, as well as the ICO's compliance with the Government Functional Standards. Both these pieces of work were presented to, and received positive feedback from, ARC. (A3)

g) Monitored progress with the ICO's risk policy and the ICO's business continuity policy and plans,. The Board receives six monthly updates and offers feedback on the actions identified in these policies and also received an update on the lessons

learned from the successful business continuity exercise which ran in May 2023. (A6)

3. Key challenges over the last 6 months

3.1. One key challenge for the Board has been to ensure that the risk review process is challenging enough to provide assurance that the register truly reflects the status of our identified risks and opportunities. The recent Regulatory Risk review work has highlighted a need to ensure risk owners use risk reviews to provide accurate, challenging and realistic assessments of the existing control environment, delivery of mitigating actions and the impact of these on risk scores.

3.2. The Board needs to ensure that its meetings do not become a 'tick box' for the work of the Risk and Governance department. A review of the proposed agenda for the July meeting of the Board, for example, highlighted that there were no agenda items that were being brought other than those that could be developed and agreed by the Director of Risk and Governance, in consultation and collaboration with relevant stakeholders. As part of our decision making framework work, we are looking at the purpose and necessity of our SLT Boards, and I would consider that Risk and Governance Board would be an area where there is potential to achieve both greater efficiency and effectiveness of decision making.

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

4.1. Three key areas of activity for the upcoming period are:

a) Input into the work being undertaken to develop a decision making framework, review of our internal governance structures and development of a culture programme to support accountability, ownership and confidence in decision making.

b) Input into work as part of the Governance Transition project, to implement governance related changes resulting from the change from a Corporation Sole to a statutory Board model.

c) Refocussing the work of the Information Risk Governance Group on ensuring that we are identifying key areas for application of our risk appetite in relation to data, compliance and security. This includes review of areas where clarity of the ICO's approach would support a more efficient DPIA process.

4.2. As above, as Chair of the Board, I will be giving consideration as to how best to engage, consult and collaborate with SLT and other stakeholders in these three strands of work.

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?

5.2. Does ET have any views on the approach being considered under paragraph 3.2?

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 (19 January 2023)

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 (19 January 2023)

A1. 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.

A2. 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.

A3. 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.

A4. 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.

A5. The Board will also make recommendations for the Audit and Risk and Committee and Management Board work programmes for 2022/3.

A6. 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.