Executive Team – for assurance

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

Meeting date: 30 June 2022

Time required: 10 minutes

Presenter: Louise Byers

Approved by: N/A

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, the oversight of information risk 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 6 January 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 January are summarised below, with a reference to the Annex where appropriate.

2.1. Oversight of the ICO's risk register, including work to ensure that the mitigating actions and target risk scores identified for our corporate risks are achievable and realistic. This work has been reported to the Audit and Risk Committee (ARC). This also includes the Board challenging risk scoring, and overseeing the identification and development of new corporate risks as well as the de-escalation of some corporate risks to directorate level.

2.2. Oversight of compliance and assurance processes, including ensuring the effective delivery of internal audit actions and reviewing internal audit reports, challenging management responses to recommendations to ensure they are robust and timescales are realistic but timely.

2.3. Reviewed and amended the 2022/23 internal audit plan prior to it being agreed by the ARC at its April meeting and also considered a three year forward look internal audit plan which is due to be presented at the June meeting of the ARC. (A4)

2.4. Considered the future provision of the internal audit service, recommending the use of the Government Internal Audit Agency to the ARC having reviewed and challenged their proposal. (A1)

2.5. Continued to challenge 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.

2.6. Oversight of the timetable for production of the Annual Report and Accounts including updates on progress and delivery. (A3)

2.7. Review of the ICO's risk appetite statement, which was then presented to, and agreed by, Management Board. (A5)

2.8. Establishment of an Information Risk Governance Group sub committee to particularly focus on the management of the ICO's information risks. This is chaired by Mike Fitzgerald and its membership covers colleagues from information governance, access, security, cyber security, facilities and IT to ensure that our information risks are being identified, mitigated and managed effectively. This sub committee will report on a 6 monthly basis to the Risk and Governance Board to provide assurance on the work in this area.

2.9. Reviewed and challenged a comprehensive paper on compliance with legal and statutory duties at the ICO, that was later presented to April's meeting of the ARC. This has been used to inform the internal audit programme, as well as the Assurance Map work that the Risk and Governance department are undertaking. (A2)

2.10. Reviewed, and recommended, the ARC work programme, that was subsequently agreed by the ARC at its April meeting. (A6)

2.11. Received and challenged reports on the business planning and business case process and lessons learnt (A7).

2.12. Received assurance regarding recent desktop incident response exercises, delivered alongside facilities and IT colleagues as well as assurance on progress on ransomware playbooks and business continuity communications plans. (A8).

3. Key challenges over the last 6 months

The key challenge for the Board over the last 6 months has been embedding and proactively communicating the organisation's risk appetite. While initial communications have gone out to staff, it has been challenging to translate the concept of risk appetite in a way that is clear, concise and meaningful for staff. Significant progress has been made by working with internal communications colleagues, and the Board expects a knowledge pack, internal training programme, case studies and other communication tools to be ready imminently to embed the risk appetite into the work of the organisation.

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

4.1. 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.

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

4.3. 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.

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

4.5. 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.

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

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

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 (6 January 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 (6 January 2022)

A1 - The Board will be considering the future provision of internal audit, looking at options to recommend to Audit and Risk Committee regarding moving from the current full outsourced model. Our preferred option is to move to the Government Internal Audit Agency (GIAA). We are currently conducting a benefits analysis of the GIAA provision to ensure that this is the best option. The current internal audit contract ends on 31 March 2023.

A2 - Further development of our Assurance Map, integrating the government Functional Standards, to then develop a compliance and assurance work programme to support the Board's second line of defence role.

A3 - 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 managing the risks identified around the change of key personnel including the Information Commissioner, the external audit provision (changing from BDO to Deloitte on behalf of NAO) and the leadership team in the Finance department.

A4 - The Board will also consider the internal and external audit plans for 2022/3 to ensure these are proportionate and prioritised effectively before they are agreed by the Audit and Risk Committee. The draft internal audit plan will also be presented to ET prior to it being presented to Audit and Risk Committee.

A5 - The risk appetite of the organisation will also be reviewed in advance of this coming to Management Board.

A6 - The Board will also make recommendations for the Audit and Risk and Committee and Management Board work programmes for 2022/3.

A7 - The Board will have oversight of the business planning process, including a lesson learned exercise to ensure continuous improvement of the approach and process, to ensure it is proportionate and delivering clear, prioritised business plans and cases.

A8 - The Board will have oversight of the continued development of our business continuity work, with a focus on the incident response plans that we will use when a business continuity event happens. One particular area of focus for this is the response potential for a potential ransomware attack. Development of this will include a desktop exercise involving ET members, during early 2022.