

## Executive Team – for assurance

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

**Meeting date:** 6 January 2022

**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.
- 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, our key governance policies and internal audit and information access performance.

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

The key achievements of the Board over the last 6 months have been:

- 2.1. Oversight of the ICO's risk register, including commissioning a full review of each corporate risk with the risk owner, focussed on ensuring the actions and mitigations identified will effectively deliver progress towards the target risk score. The Board also commissioned an annual review of the risk register to help track progress across the risk register, as well as work to identify interdependencies between risks to help the ICO effectively plan for a scenario where multiple risks crystallise. This work has also been presented to Management Board and the Audit and Risk Committee.
- 2.2. Oversight of compliance and assurance processes, including the effective delivery of internal audit actions, tracking progress, in particular where agreed timescales have proved challenging.
- 2.3. Continued assurance of the ICO's cyber security defences and approach, to ensure these are benchmarked against best practice

and industry standards, as well as regular review of the ICO's cyber security dashboard.

- 2.4. The Board commissioned a review of other public bodies' key governance documents to highlight good practice and ensure our approaches are benchmarked against other ALBs and regulators. The learning from this work has been shared with those leading on our change and transition work, our annual report development and finance colleagues.
- 2.5. Introducing a new assurance mechanism for the publication of financial transparency information to ensure the Risk and Governance Board has oversight of this area.
- 2.6. Review and updating of the Scheme of Delegation to reflect changes in the organisation, as well as regulatory and statutory obligations.
- 2.7. Review of our compliance with various standards, including those relating to cyber security and the Government's Functional Standards.
- 2.8. The approval and laying of the ICO's Annual Report, ensuring a focus on the ICO's key outcomes in the period as well as its governance and financial performance.

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

The key challenges for the Board over the last 6 months have been:

- 3.1. The Board has led on oversight of the performance of the Information Access team. The impact of the pandemic, as well as increasing profile and interest in the work of the ICO, has led to a backlog of cases, including those which have gone beyond the statutory deadlines for response. The Board have monitored the impact of the late cases project, as well as the wider recovery plan to ensure we return to our service standards. Over the period, significant progress has been made on reducing the number of overdue cases, as well as the overall caseload. The Board are aware that ET and SLT colleagues have supported this effort, through sharing services (for example, initial sift and triage of cases) as well the provision of additional resources to support the delivery of the recovery plan.
- 3.2. Bringing together, and embedding, risk management, governance and decision making from across the organisation, to ensure corporate and regulatory decision making is informed by the

organisations risk appetite and risk profile. The Board has kept up to date with the regulatory risk and governance work through regular updates from its members, but ensuring a joined up and consistent approach to governance, decision making and risk across the organisation has proved particularly challenging in a time of remote working coupled with ongoing organisational growth.

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

- 4.1. 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.
- 4.2. 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.
- 4.3. The delivery of the 2021/22 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.
- 4.4. The Board will also consider the internal and external audit plans for 2022/23 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.
- 4.5. The risk appetite of the organisation will also be reviewed in advance of this coming to Management Board.
- 4.6. The Board will also make recommendations for the Audit and Risk and Committee and Management Board work programmes for 2022/23.

- 4.7. 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.
- 4.8. 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.

## 5. Areas for challenge

- 5.1. ET may wish to consider whether the role of the Risk and Governance Board is clear and whether the level of assurance that the Board provides to the Executive Team through the reports to Management Board and Audit and Risk Committee is sufficient.
- 5.2. The approach to risk and embedding this into the decision-making processes of the organisation can be improved. ET may wish to consider how we drive the use of risk appetite across the organisation and be clear to our teams about the parameters in which we work.
- 5.3. 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?

**Author:** Louise Byers

**Consultees:** Corporate Governance Team.

**List of Annexes:** None

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