# Risk and Governance Board (RGB) terms of reference

## 1. Purpose

1.1. The overall purpose of the SLT Boards is to deliver SLT's purpose of strategic oversight and delivery of cross-office priorities and plans. The Boards were created to ensure that sufficient capacity within these meetings for consideration, challenge, and scrutiny to deliver SLT's collective role.

1.2. The Risk and Governance Board (RGB) is tasked with assisting the Information Commissioner and Senior Leadership Team with the governance of the organisation and management of risk to achieving its strategic priorities and service delivery. It will achieve this purpose by reviewing all matters concerning the development, maintenance and implementation of the ICO's risk and governance management frameworks, including monitoring and reporting arrangements.

1.3. Members of the RGB are expected to be a catalyst for embedding and strengthening risk and governance management in corporate business processes through their role.

## 2. Responsibilities

2.1. The RGB is responsible for:

- Providing the formal second line of defence within the ICO's risk management framework through oversight of risk management, including the review of risk registers, monitoring of significant strategic, operational and cross-cutting risks, approving risk escalation and ensuring the alignment of risk management activities and regulatory priorities. Seeking assurance on the effectiveness of risk mitigation from risk owners, ensuring consistency of scoring and mitigation of risks throughout the organisation in line with the ICO's risk appetite.
- Ensuring that risks highlighted through the ICO's various risk management tools and techniques are managed appropriately.

- Oversight of internal control, governance and compliance culture issues, including review of representatives on external bodies or organisations, openness and transparency, and organisational compliance.
- Oversight of the effectiveness of, and compliance with the organisation's business planning and performance management processes.
- Oversight of the effectiveness of the ICO's business continuity planning, preparedness and resilience.
- Overview and scrutiny of information governance (IG) arrangements and for making recommendations to the Senior Information Risk Owner (SIRO) on information governance decisions.

2.2 The RGB is also responsible for ensuring that equality, diversity and inclusion (EDI) considerations are continually considered and addressed throughout the ICO's work. The RGB is also responsible for ensuring the delivery of the ICO's equality objectives (within the RGB's remit). The Board may refer issues to the EDI Board as appropriate, and consider issues referred to it by the EDI Board.

## 3. Work Programme

3.1. The RGB will maintain a work programme which sets out its expected activities to meet these responsibilities for the next 12 months. The RGB will consider this work programme at each meeting. Corporate Governance will keep this work programme up to date based on the information provided by Board members.

## 4. Authority

4.1. The RGB derives its authority from ET and SLT. Where work of the Board is materially contributing to achieving ET's goals, the Board will report this to ET for assurance. Where the work of the Board introduces a significant risk to achieving ET's goals, the Board will refer that to the relevant ET member, who may refer this to ET for decision. ET's goals are provided as an annex to these Terms of Reference.

## 5. Reporting to other bodies

Senior Leadership Team

5.1. The Chair of the RGB Board will provide a report on the Board's activities to each meeting of SLT. This include highlighting any

issues to be discussed at future Board meetings, to facilitate advanced consultation. The RGB's work programme will also be provided to each SLT meeting for information.

5.2. Where required, other members of the Board may attend SLT meetings to provide information or input from the RGB.

Other Boards

5.3. The RGB will work collaboratively with the other Boards as appropriate, ensuring that views of other Boards are considered when the RGB exercises its responsibilities, and understanding that other Boards will act similarly in considering the RGB's views. This may happen at an informal level between Board Chairs or Board members.

5.4. The RGB will highlight issues to SLT or refer issues to other Boards for information where it is clear that another Board should be aware of the work of the RGB.

5.5. There is no overlap between the roles of the Boards. However, in exceptional circumstances, there may be issues where approval is required by more than one Board before action can be taken. This should be avoided wherever possible through discussion between Board chairs and consultation between Board members. However, where this is unavoidable, the same report should be reframed and presented to both Board meetings, with a clear recommendation on the specific decision needed from each Board. Outcomes from one Board will be reported to the other Boards. Corporate Governance will facilitate this process.

5.6. In the event of a conflict between two Boards, the Chairs should meet to determine the way forward and inform Corporate Governance accordingly. If conflict remains, the matter should be referred to SLT for decision.

Programmes

5.7. The RGB may be responsible for the delivery of a range of programmes. These will be delivered through a separate programme board, but as required this programme board will report to the RGB to ensure appropriate oversight.

Executive Team

5.8. The RGB may refer issues to ET where they require clarity, direction and approval in areas of greatest corporate risk or opportunity.

Management Board

5.9. Minutes of RGB meetings will be presented to the Management Board for information.

## 6. Chair

6.1. The RGB is chaired by the Director of Risk and Governance. When the chair is unavailable for a meeting, they will nominate a substitute to chair the meeting in their absence.

## 7. Composition

7.1. The members of the RGB are:

- Chair (Director of Risk and Governance)
- Director of Digital, IT and Business Services
- Director of Legal Services (Regulatory Enforcement)
- Director of People Services
- Director of International Regulatory Cooperation
- Director of Investigations
- Director of Governance Transition
- Head of Risk and Governance
- Head of Cyber Security

7.2. The Chair may amend this membership as required. They will report this to the next meeting of the Board when doing so, including the reasons for the change in membership. Corporate Governance will then update the Terms of Reference.

7.3. The Chair will invite the risk owners for significant strategic or operational risks for meetings where the risk they own require discussion

7.4. The Chair may also invite any other ICO staff to RGB meetings as required. This may include Chairs of other Boards, where an issue with crossover to that Board's area of responsibilities is due to be discussed.

7.5. As set out in the purpose statement, members of the RGB are expected to be a catalyst for embedding and strengthening risk and governance management in corporate business processes through their role.

## 8. Quorum

8.1. The quorum is:

- The Chair (or their nominated substitute); and
- At least three other members, including any corporate risk owners.

## 9. Information requirements

9.1. All RGB members are responsible for ensuring that appropriate information is provided to the RGB to complete its responsibilities, including appropriate consultation to ensure that all potential impacts are considered before decisions are made. The Chair is ultimately responsible for determining what information is required.

## 10. Budget

10.1. The RGB has no specific budget. Any work commissioned by the Board will be funded from budgets within the relevant Directorate(s), or funded through an approved business case where necessary. This should be exercised in accordance with other ICO budget controls.

## 11. Secretariat

11.1. Secretariat is provided by the Corporate Governance Team.

## 12. Frequency of meetings

12.1. The Board should meet every six weeks.

## 13. Decision-making between meetings

13.1. In the event that an urgent decision is required between meetings, the RGB may consider reports by correspondence, particularly those reports not likely to require significant discussion. Corporate Governance will facilitate this.

13.2. Any reports considered on this basis must receive sufficient responses to constitute the quorum for an RGB meeting. RGB members will usually be given one week to consider reports circulated by email, but if a clear consensus emerges before that, the decision may be implemented sooner. If significant discussion is required, the report should be referred to the next RGB meeting.

13.3. Corporate Governance will provide a report to each RGB meeting on any matters considered by email, the comments received and the outcome of the consideration.

## 14. Evaluation

14.1. The RGB should ensure that arrangements are in place to enable it to discharge its responsibilities effectively, including a formal annual evaluation of the RGB's performance. Action should be taken according to outcomes.

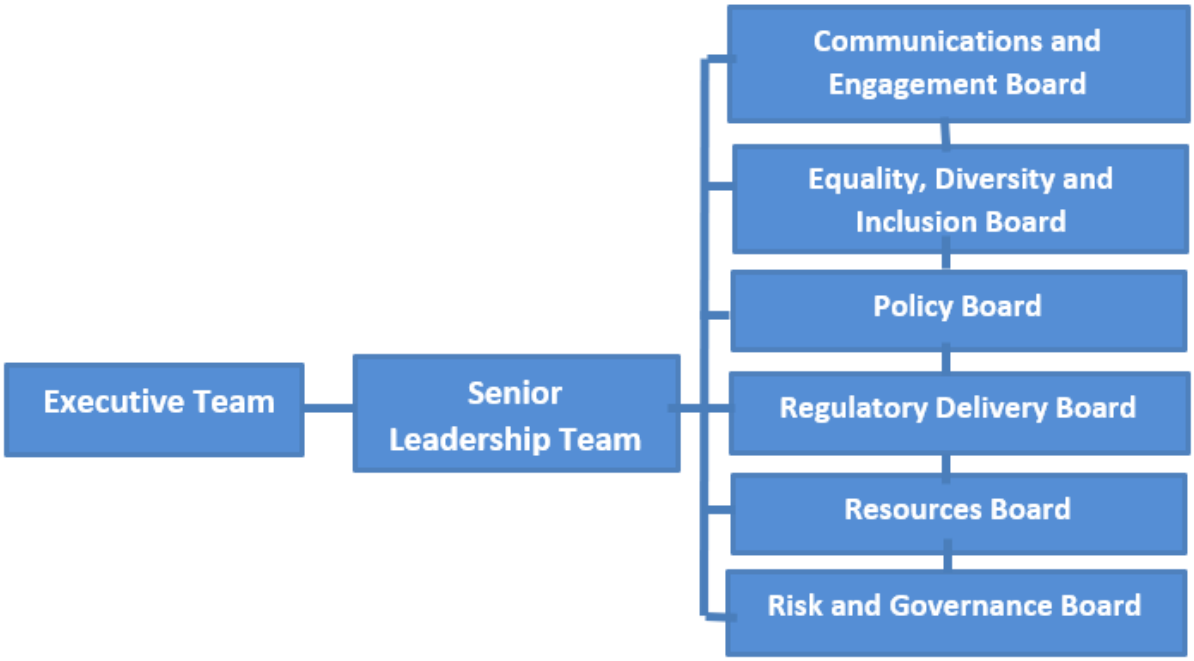
## 15. Publication of papers

15.1. The agenda for each meeting will be published internally via SharePoint. The minutes will be published internally via SharePoint, once approved. Reports will be published internally via SharePoint where deemed appropriate by report authors.

15.2. Agendas, minutes and reports will not be published externally.

## 16. Links to other forums

16.1. The Board's place in the overall governance structure is set out in the diagram below.




## Annex – Executive Team goals

- Position of the organisation as the information rights regulator – setting the vision and mission and ensuring that all activities, either directly or indirectly, contribute towards it. Long-term horizon scanning, ensuring the strategic direction is based on a collective understanding of policy issues; using outside perspective to ensure that the ICO is challenged on its outcomes and understanding the

perspective of others, in particular the regulated community and the public.

- Setting the tone and culture of the ICO – setting the ICO's risk appetite and ensuring controls are in place to manage risk; agreeing and monitoring the ICO's people related strategies and plans, monitoring the organisation's compliance culture and ensuring there is a clear vision for the way the ICO works and understanding of its values.
- Ensuring the ICO has the capacity and capability it needs - determining sign-off of large operational projects or programmes; ensuring sound financial management; scrutinising the allocation of financial and human resources to achieve the plan and ensuring organisational design supports attaining strategic objectives. Evaluation of the Board and its members and succession planning to ensure the ICO has the capability to deliver and to plan to meet current and future needs.
- Defining the perception of the ICO – agreeing plans and strategies; setting objectives for strategic engagement activities; driving the ICO to be an effective, modern, independent regulator.
- Monitoring the performance of the ICO towards achieving its strategic goals – ensuring clear, consistent, comparable performance information is used to drive improvements and demonstrate the impact of the work of the organisation. Monitoring and steering performance against plan; scrutinising performance and setting the ICO's standards and values, holding the Executive to account for delivery of its plans and strategies.