Management Board – for assurance

Meeting agenda title: Corporate Risk and Opportunity Register – annual progress report

Meeting date: 13 December 2021

Time required: 10 minutes

Presenter: Louise Byers

Approved by: Paul Arnold

1. Objective and recommendation

1.1. This report provides the Management Board with an overview of progress and changes in the corporate risk and opportunity register (corporate risk register) over the last 12 months.

2. History and dependencies

2.1. At its May 2021 meeting, the Board requested that it receive this report on an annual basis, rather than considering the corporate risk register at every meeting. The corporate risk register is considered by the Audit and Risk Committee and the Risk and Governance Board all of their meetings.

3. Developing a common understanding

3.1. The corporate risk register sets out the risks and opportunities which have the most fundamental impact on the ICO's ability to achieve its corporate objectives. Risks and opportunities are described as a cause, threat and impact, with the impact being primarily described in the context of the relevant IRSP objectives.

3.2. Risk and opportunities are scored out of five for likelihood. These scores are then multiplied together to provide the overall score. Opportunities are scored inversely to risks: a low score for an opportunity indicates that the opportunity is not being exploited very well, while a low score for a risk indicates that the risk is being mitigated very well.

3.3. The corporate risk register is supported by Directorate risk registers, which are developed as part of Directorate business plans. Risks may be escalated to the corporate risk register from Directorate risk register or relegated from the corporate risk to Directorate risk registers.

4. Matters to consider to achieve objective

4.1. Management Board reviewed the ICO's risk appetite in February 2021. The Board kept the risk appetite statement broadly the same, with the only changes being amendments to the descriptions of the various parts of the regulatory risk appetite, clarifying the categories of "regulatory evaluation", "regulatory investigation" and "regulatory enforcement and intervention". The Board will be asked to review the risk appetite again in March 2022.

4.2. In comparison to the risk register which was presented to the Management Board meeting in November 2020, the following changes have occurred to corporate risks:

- No risk scores increased from November 2020 to November 2021.
- Three risk scores decreased from November 2020 to November 2021 (R46: Financial Resilience; R84: Major Incident; R87: International Position).
- Four risks added to the risk register (R90: Regulatory Action; R91: Targeted regulatory activity; R92: ICO Guidance; R93: Online safety)
- Two risks de-escalated from the corporate risk register to Director risk register (R10 Statutory Codes; R29: Technology Relevant Regulator)
- One risk combined into a new corporate risk (R76: Cyber Security Regulation)
- Two risks changed to opportunities (O2: Service Excellence; O71: Online Safety).

4.3. We currently have three risks with red ratings, compared to five rated as red in November 2020. Overall, the average score of risks on the corporate risk register has reduced from 10.8 in November 2020 to 10.2 in November 2021. This paints a picture of our overall risk environment being relatively similar to the same time last year, if slightly decreased. Given the areas of uncertainty which have existed throughout the year (particularly the ongoing COVID-19 pandemic, data protection reform, recruitment of a new Commissioner), the current risk register reflects the work to keep our risk profile relatively static in the face of significant external

uncertainty. The end of the EU Withdrawal process and the completion of the transition period for the Children's Code did reduce a couple of significant areas of uncertainty and risk.

4.4. Details of the changes to each of the risk on the corporate risk register are provided at Annex 1. The highest rated risk on the register is R4 (Capacity and Capability). This risk has remained as a score of 20 and the highest rated risk on the register throughout the year. Given the continuing importance of this risk, we are currently in the process of splitting it into two separate risks, one covering capacity and one covering capability. This should make it easier to identify controls and future actions for both risks, as it will be easier to accurately target the mitigations towards either capacity or capability. These changes are currently being finalised and we will present the updated risks and mitigations to the Audit and Risk Committee in January 2022. The proposed risk descriptions are set out below:

- Capacity risk: (Cause) increasing demand, expectations and/or unplanned work results in (Threat) insufficient and/or overstretched resources (particularly in specialist roles) that are unable to deliver all business requirements creating operational issues and pinch points (impact) impacting on the ICO's ability to deliver all of its corporate objectives.
- Capability risk: (Cause) the ICO does not have appropriate capability to ensure it is able to deliver its regulatory remit and responsibilities (particularly in specialist areas) (Threat) leading to the ICO facing issues in supporting organisations to establish good practices in data protection, and repeated successful challenge to enforcement action resulting (Impact) in reputational harm and impacting the ICO's ability to demonstrate that it is an effective and knowledgeable regulator.

4.5. Looking ahead, it is likely that the key event on the horizon which will affect the ICO's risk landscape is the data protection reform work with DCMS. This is likely to have a direct impact on many of the top risks on the risk register, particularly O3 (Expectations Gap), R85 (Managing ICO reputation) and R88 (future role of the ICO), plus an indirect impact on many other risks. It is also likely that there will be a larger-than-usual amount of change in the risk

register during the coming year; when the new ICO plan is finalised, we will identify the risks to achieve the strategic objectives set out in that plan, which may well lead to a large degree of turnover in the risk register.

4.6. Prior to this report being presented to Management Board, it was considered by the Risk and Governance Board (RGB). RGB's main focus was on the level of assurance that was provided that the risks were being actively managed and mitigated, via the completed and future mitigation actions which are identified on the risk register. In response to this, the Risk and Governance Team reviewed all of the mitigating actions in the corporate risk register and met with the owners of each of the corporate risks and opportunities to ensure that these substantially mitigated the score of the risk (that on its own, each action either reduces the score, or stops the score from increasing). The Risk and Governance Team and risk owners also worked with the Business Planning team to ensure that all future mitigating actions are reflected in Directorate Business plans. This will ensure that there is a clear focus on delivering these key actions.

4.7. We have also closely reviewed the interdependencies between risks, so that we can identify all risks which will need to be reviewed if a risk turns into an issue. We have identified the interdependent risks and have created a matrix to identify which other corporate risks would increase were each of the risks to materialise. This means that we can ensure that the ICO has a clear view of its over risk environment and how to manage the wider impacts of a risk materialising.

4.8. We are also in the process of recruiting a new post within the Corporate Governance Team of Risk and Business Continuity Manager. This post will provide more resources to support risk owners at all levels in identifying and mitigating risk, which will increase the risk maturity of the whole organisation. We hope to have this post filled in early 2022.

5. Areas for challenge

5.1. Does this report demonstrate the level of progress that the Board would expect to see in mitigating risks over the last year? Does the annex provide sufficient detail for Management Board on how risks have developed over the last year?

6. Next steps

6.1. The next steps for this work are:

- Continue to deliver the actions to mitigate the existing risks on the corporate risk register, including reviews at each meeting of the Audit and Risk Committee and Risk and Governance Board.
- Management Board to review the risk appetite in March 2022.
- Review the risk register once the new ICO Plan has been developed, to identify the risks to achieving those corporate objectives.
- Produce the next iteration of this report for Management Board in November 2022.

Author: Chris Braithwaite

Consultees: Louise Byers, Joanne Butler, Caroline Robinson, Risk and Governance Board

List of Annexes: Annex 1 – Corporate Risk Register updates since November 2020

Annex 2 – Corporate Risk and Opportunity Register

Publication decision: The report and Annex 1 can be published internally and externally without redactions. Annex 2 (the corporate risk register) can be published with appropriate redactions.

Outcome reached: