Audit & Risk Committee – for decision

Meeting agenda title: Corporate Risk and Opportunity Register Review

Meeting date: 10 January 2022

Time required: 10 Minutes

Presenter: Louise Byers

Approved by: Louise Byers

1. Objective and recommendation

1.1. The objective of this report is for the Audit and Risk Committee to consider recent updates to the Corporate Risk Register and Opportunity Register, following the latest iteration of the Corporate Risk Review.

1.2. The Audit & Risk Committee are recommended to note the report.

2. Developing a common understanding

2.1. Prior to this report being presented to the Audit and Risk Committee, 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. As a result all existing and planned actions have been reviewed and all future actions have been confirmed as included in Directorate business plans, to ensure that these would be completed.

3. Matters to consider to achieve objective

Risk Review

3.1. To support the approach outlined above, for this iteration of the risk review the Corporate Governance team met with each of the risk owners to assist them in completion of the risk review. This led to a more thorough and targeted review of the risks, and also meant that we were able to directly feed the comments from Risk and Governance Board into the review. While this was more resource-intensive, it was worthwhile and we will repeat this for future iterations of the review.

3.2. 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.

3.3. The existing controls, risk indicators, future planned actions and risk scores were reviewed and amended as appropriate, with a particular focus on ensure that the actions material mitigate the risk. The key issues emerging from those reviews are as follows:-

- R90 (Regulatory Action & Activity) : this risk was reviewed in conjunction with R91 (Targeted Regulatory Activity) and as a result has been renamed with the risk description slightly amended to take into account the cross over with R91.

  Having reviewed the existing controls it was agreed to reduce the current risk rating to 9 (likelihood 3 x 3 impact) as the controls and methodologies that are currently in place provide added assurance on processes and accountability of decision making and thereby reduces the likelihood of the risk.

- R91 (Targeted Regulatory Activity) : Due to the similarities with R90 (Regulatory Action) it was proposed that we dormant R91 from the Corporate Risk Register. However we would expect this risk to be recognised on relevant director risk registers as a cause and threat of the risk covered in the updated R90 which has been renamed Regulatory Action and Activity.

- R73 (Compliance Culture): Following discussions at the October Audit & Risk Committee meeting and a review of the existing controls and future planned actions, it was recommended that the current risk score be increased to 16 (likelihood 4 x 4 impact). Whilst it is recognised that the organisation has improved its compliance and accountability culture, there are a number of actions still to be undertaken within some areas of the organisation to ensure sufficient assurance of compliance.
- O71 (Online Safety): It was recommended to deescalate this Opportunity and it will be managed within the directorate risk register.
- O2 (Service Excellence): It was recommended that the current risk rating be increased to 9. It was recognised that although the future planned actions will be implemented over the next 2-3 years we should see incremental improvements during this time.
- R86 (Political & Economic Environment): During the review it was recommended that all the risk ratings should be increased including the current risk rating from 6 to 9 (likelihood 3 x 3 impact). It was agreed that although the likelihood of the risk occurring could be reduced by the existing controls in place, the impact would remain at medium.
- R4 (Capacity & Capability): The articulation of this risk has been reviewed and we are planning that the risk be split as follows:-

  R4a (Capacity) : **Capacity** (Cause) our workforce planning approaches means that we do not match staff supply to the demand and expectations which results in (Threat) insufficient and/or overstretched resources (particularly in specialist roles), insufficient capacity to prioritise unplanned work 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 as well as impacting on staff wellbeing and welfare.

  R4b (Capability) : **Capability** (Cause) our workforce planning, evaluation and development approaches means that we do not have clear plans on how to identify gaps or develop appropriate capability (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 (impact) resulting in difficulties in delivery of our regulatory remit, reputational harm and impacting the ICO’s ability to demonstrate that it is an effective and knowledgeable regulator

3.4. The tables below informs the Audit & Risk Committee on progress against key risks, please note for threats the highest rated are highlighted in the highest rated table and for opportunities the lowest scoring is highlighted. This is because the scoring mechanism is reversed for threats and opportunities (threat risks we wish to reduce the score, opportunity risks we wish to increase the score). **Annex 1** shows a heat map of the threats and opportunities.

Table 1: Highest Rated Corporate Risks

Ref	Type	Risk Title	Rating	Direction
R4	Threat	Capacity and Capability	20 High	Static ↔
R73	Threat	Compliance Culture	16 High	Up ↑
O3	Opp’ty	Expectations Gap	4 High	Static ↔

Table 2: Risk Watch List

Ref	Type	Risk Rating	Rating	Direction
R46	Threat	Financial Resilience	12 Med	Reducing ↓
R83	Threat	Staff Welfare and Wellbeing	12 Med	Reducing ↓
R84	Threat	Major Incident	12 Med	Static ↔
R61	Threat	Litigation Resource	12 Med	Static ↔
R72	Threat	SMEs	12 Med	Static ↔
R88	Threat	Future role and structure of ICO	12 Med	Static ↔
R89	Threat	Compensation	12 Med	Static ↔

<u>Consultation done or needed</u>

3.5. The risk owners for each of the risks on the Corporate Risk Register were consulted in relation to this review.

4. Areas for challenge

4.1. Are the actions identified sufficient controls to ensure that they mitigate the risk and are able to materially change the risk scores?

4.2. Are the interdependencies identified for the each of the risks the correct ones?

5. Communications considerations

5.1. Risk owners will need to be informed of any recommended changes to corporate risks from this Board. Corporate Governance will inform risk owners accordingly.

6. Next steps

6.1. The next steps for this work are:

- Commence the next iteration of the risk review, which will be reported to the Risk & Governance Board's March meeting. This will consider the following risks:
  - R93 (Online Safety)
  - R73 (Compliance Culture)
  - R85 (Managing ICO Reputation)
  - R87 (International Position)
  - R83 (Staff Wellbeing and Welfare)
  - R21 (Cyber Security)
  - R72 (SMEs)
  - R92 (ICO Guidance)
  - R89 (Compensation)

6.2 To review the format of the risk register and supporting information to ensure it is accessible and gives the right level of detail to inform discussion.

6.3 Management Board to review the risk appetite in March 2022.

6.4 Review the risk register once the new ICO Plan has been developed, to identify the risks to achieving those corporate objectives.

Author: Caroline Robinson

Consultees: Chris Braithwaite, Joanne Butler

List of Annexes:

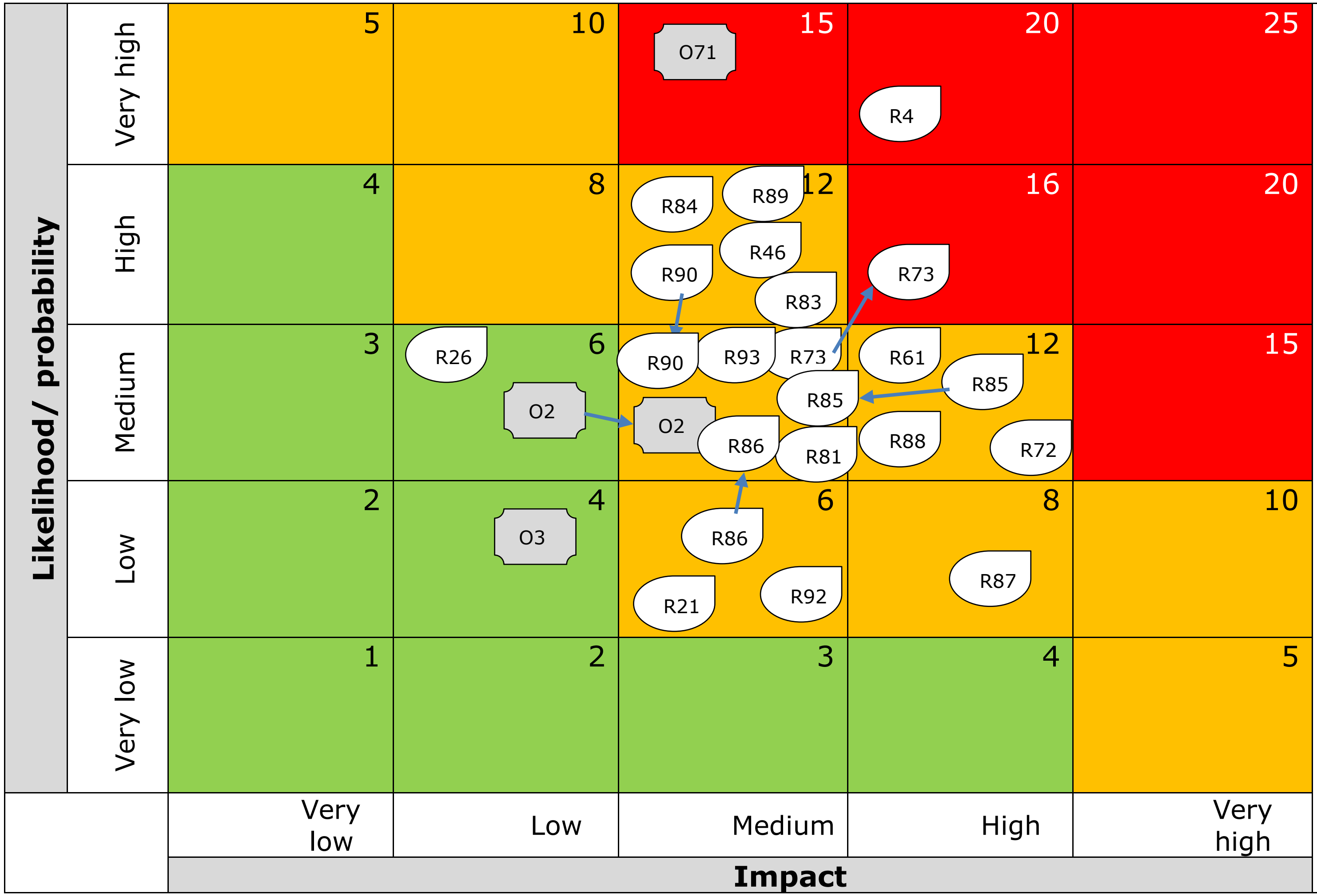
Annex A – Risk Heat Map

Annex B – Risk & Opportunity Interdependencies

Publication decision: This report can be published externally and internally without redactions

Outcome reached:

Annex A: Risk Heat Map



Likelihood/ probability	Very low	Low	Medium	High	Very high
Very high	5	10	15 O71	20 R4	25
High	4	8	12 R84 R89 R46 R90 R83	16 R73	20
Medium	3	6 R26 O2	R90 R93 R73 O2 R85 R86 R81	12 R61 R85 R88 R72	15
Low	2	4 O3	6 R86 R21 R92	8 R87	10
Very low	1	2	3	4	5
	Impact				

- R4: Capacity and Capability
- R21: Cyber Security
- R26: Improving productivity
- R46: Financial Resilience
- R61: Litigation Resource
- R72: SMEs
- R73: Compliance Culture
- R81: Management Board Resilience
- R83: Staff Wellbeing
- R84: Major Incident
- R85: Managing ICO Reputation
- R86: Political and Economic Environment
- R87: International Position
- R88: Future Role and structure of ICO
- R89: Compensation
- R90: Regulatory Action & Activity
- R92 ICO Guidance
- R93: Online Safety
- O3: Expectations Gap
- O2: Service Excellence
- O71 Online Safety

Note: scores for opportunities are the inverse of scores for risks and should travel from low to high as the opportunity is exploited. So opportunities in the green section of the heat map are being exploited poorly and opportunities in the red section are being exploited well.