Meeting:	Audit Committee	**Date:**	21 June 2021
Agenda item:	10	**Time:**	15 minutes
For decision			
Presenter:	Joanne Butler		

1. Topic

1.1. Risk and Opportunity Register

2. Issue

2.1. To provide the Audit and Risk Committee with assurance on the ICO's corporate risk and opportunity register.

3. Reason for report

3.1. Audit and Risk Committee review the ICO's corporate Risks and Opportunities at each meeting as part of its formal risk and assurance governance function.

4. Overview of updates to the corporate risk register

4.1. Corporate risks are subject to a full review by the Risk and Governance Board on a bi-monthly basis, with the most recent review having taken place in May 2021.

4.2. Since the Audit and Risk Committee last met in April 2021, the following amendments have been made to the risk and opportunity register:

a) R46: Financial Resilience: The Risk and Governance Board considered whether to reduce the current likelihood of this risk from 4 to 3 (and the current score from 16 to 12). This would have been to reflect the fact that for 2021/22 the income growth projections are spread more evenly throughout the year and rigorous monthly reviews of expenditure will ensure that any variances can be highlighted earlier within the year and managed accordingly. However, the Board agreed that while there was a reduced risk of insufficient funding during 2021/22, due to the complexity of the 2021/22 budget there

was an increased risk of underspend, which may have a reputational impact.

Therefore, the Board agreed that the description of this risk should be reviewed to ensure that it reflects the risk of both insufficient funding and insufficient expenditure. The risk is now described as:

"Financial Resilience: (Cause) Risk that sensitivities in the income growth forecast and new territories of expenditure (threat) create inaccurate financial forecasting and planning assumptions (impact) leading to insufficient funding or over-funding and financial stress and impacting the ICO's reputation, its ability to meet its statutory requirements, and full delivery of all of its intended IRSP goals and outcomes."

The current score of this risk remains at 16. The risk will be regularly reviewed during the year to ensure that the rating remains accurate.

b) R87: International Position: The likelihood of this risk occurring has been reduced from 3 to 2. This reflects the European Commission issuing a draft adequacy decision and although there is some continued risk of an adequacy gap due to a delay as a result of a UK Court of Appeal ruling, the ICO now has well developed approaches to international engagement in the context of GPA and on issues related to the Covid-19 pandemic. The current score of this risk is therefore 8 which is medium risk but this risk will be reviewed again at the end of June (the end of the data bridge period).

4.3. In addition, the following matters will be considered during the next iteration of the risk review. At the time of writing, this is currently ongoing, and is due to be considered by the Risk and Governance Board at its meeting on 29 June. Any emerging outcomes will be reported to the Committee if available.

a) R10: Statutory Codes: the Directors responsible for the production and delivery of the various statutory codes will meet to review the wording of this risk. This is required as the risks are at different stages of development and it is necessary to consider whether having a single corporate risk is appropriate to manage the risks. The alternative would be to divide this risk into multiple risks for each individual Code, with these risks being held within Directorate risk registers.

b) R73: Compliance Culture: This last iteration of the risk review coincided with the Audit and Risk Committee considering the compliance report (at its last meeting). In the next iteration of the risk review the phrasing of this risk will be reviewed to ensure it appropriately captures the current compliance position.

c) O71: Online Safety: The previous iteration of the risk review was conducted prior to the Queen's Speech, so this opportunity will be reviewed again in the next iteration of the review, to ensure that the opportunity is up to date.

d) R4: Capacity and Capability: This risk will be reviewed in light of an increasing number of asks re our future remit and clarity on additional resources required in time to support the work.

5. Update on risk maturity action plan:

5.1. Since the last update to the Committee, the new Risk and Governance Board (RGB) has become embedded in to the ICO's governance structure, providing a formal second line of defence within the ICO's risk management framework through oversight of risk management, including the review of risk registers, and ensuring the alignment of risk management activities and regulatory priorities. The Board also seeks 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.

5.2. As part of the Business Planning process, Directorates are developing Directorate Risk Registers, to ensure that any risks to achieving Directorate objectives are identified and appropriately managed. The Risk and Governance Team will also use these Directorate registers to identify any cross-cutting risks or opportunities which may need managing across Directorates. We will also be developing processes to escalate risks from Directorate registers to the corporate risk register if they are fundamental risks to achieving our corporate objectives.

6. Heat maps

6.1. The tables below inform the 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 A** 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	Static ↔
R83	Threat	Staff Welfare and Wellbeing	16 High	Static ↔
R46	Threat	Financial Resilience	16 High	Static ↔
O3	Opp'ty	Expectations Gap	4 High	Static ↔

Table 2: Risk Watch List

Ref	Type	Risk Rating	Rating	Direction
R84	Threat	Major Incident	12 Med	Static ↔
R10	Threat	Statutory Codes	12 Med	Static ↔
R61	Threat	Litigation Resource	12 Med	Static ↔
R72	Threat	SMEs	12 Med	Static ↔
R85	Threat	Managing ICO Reputation	12 Med	Static ↔
R90	Threat	Regulatory Action	12 Med	Static ↔
R88	Threat	Future role and structure of ICO	12 Med	Static ↔
R89	Threat	Compensation	12 Med	Static ↔

7. Deep dives

7.1. At each meeting, the Committee is given the opportunity to identify any of the risks on the register to be subject to a "deep dive" at the Committee's following meeting. This will take the format of a short briefing and opportunity for questions to the risk owner of that specific risk. There is no requirement that the Committee conduct a "deep dive" at each meeting if it does not wish to do so.

8. Recommendations

8.1. Audit and Risk Committee is recommended to note the risk register and, if desired, identify a risk for a "deep dive" at the October 2021 meeting.

9. Alignment with values

9.1. Reviewing the risk register and ensuring that risks to our corporate objectives are being managed helps to ensure we are being ambitious and service focused. It also assists in ensure we focus our collaboration in areas which have the most value in mitigating and managing risk.

10. Link to the Information Rights Strategic Plan

10.1. The risk register helps to prioritise and track actions against all the IRSP.

11. Publication considerations

11.1. This report can be published internally and externally. The corporate risk register is published internally, and externally with redactions where appropriate.

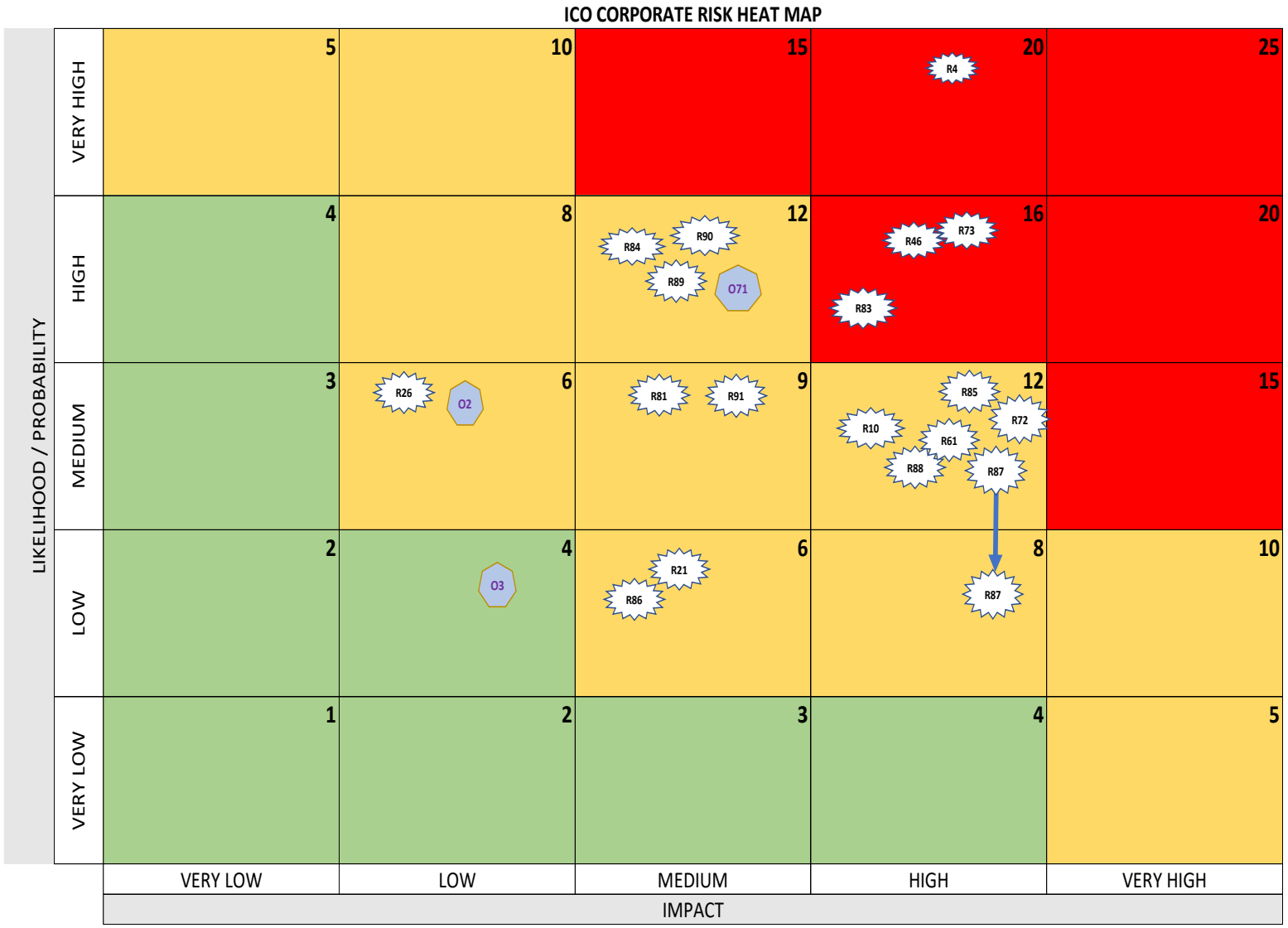
Author: Chris Braithwaite

Consultees: Jo Butler, Louise Byers

List of Annexes: Annex 1 – Heat map

Annex 2 – Corporate Risk and Opportunity Register

Annex A: Risk Heat map



Current Scored Risks Key:

R4: Capacity and Capability (Th)
R73: Compliance Culture (Th)
R46: Financial Resilience (Th)
R84: Major Incident (Th)
R85: Managing ICO Reputation (Th)
R90: Regulatory Action (Th)
R10: Statutory Codes (Th)
R61: Litigation Resource (Th)
R88: Future Role and Structure of ICO (Th)
R83: Staff Wellbeing and Welfare (Th)
R72: SMEs (Th)
R87: International Position (Th)
R89: Compensation (Th)
R91 Targeted Regulatory Activity (Th)
R81: Management Board Resilience (Th)
R26: Improving Productivity (Th)
R21: Cyber Security (Th)
R86: Political and Economic Environment (Th)

O3: Expectations Gap (Opp)
O2: Service Excellence (Opp)
O71: Online Safety (Opp)