Audit and Risk Committee – for decision

Meeting agenda title: Three Year Internal Audit Plan

Meeting date: 20 June 2022

Time required: 10 minutes

Presenter: Louise Byers

Approved by: Paul Arnold

1. Objective and recommendation

1.1. For the Audit and Risk Committee to agree areas for inclusion on a draft three-year draft Internal Audit Plan for 2023/24 onwards.

2. History and dependencies

2.1. Currently, the ICO's internal audit function is provided by Mazars. A plan of internal audits for the financial year 2022/3 was approved by the Audit and Risk Committee in April.

2.2. Normally, in developing the internal audit plan any given year, the auditors also provide an indicative audit plan for upcoming years – usually three years ahead. This allows the Committee to understand the wider picture of the assurance it will receive over a longer period of time. This assurance informs its opinion on the internal control environment that is included in the Annual Report each year.

2.3. At its last meeting, the Committee asked for a plan to developed through to 2024/5. This paper sets out a proposal for a three year audit plan for the Committee to discuss and agree.

2.4. This plan will also provide a helpful steer when we consider the procurement of new internal audit services for 2023/4 onwards and we will use it as an indication of the areas of assurance we would consider to be a priority.

2.5. As a reminder, the agreed audits for 2022/23 are:-

- Cyber Security
- Risk Management
- Core Financial Controls – Corporate Charge Card
- IT Strategy
- Guidance Development

- People Strategy
- Procurement and contract management

2.6. Annex A sets out the internal audits delivered since 2018/9.

2.7. Of course, it is challenging to anticipate new and emerging risks and areas of interest. This is especially true at a time of significant external (political, economic and social) uncertainty and during a period that will see a new ICO strategic plan and DP reforms. However, the ICO's compliance report (reviewed at the April Audit and Risk Committee meeting) the corporate risk register and the government functional standards (Functional Standards - GOV.UK (www.gov.uk)) provide a starting point for consideration of areas of focus for internal audit assurance.

2.8. There is also flexibility in the internal audit plan, either though re-prioritising audits, or using extra audit days, as necessary if additional areas are identified. It is also anticipated that when we reprocure the internal audit service, additional days will be included to ensure we can cover the full range of internal controls assurance work necessary given the growth of the ICO since the start of the current contract.

2.9. There are also helpful external sources which can inform future areas of assurance, for example the Institute of Internal Auditors OnRisk report for 2022: 2021-2865-onrisk-report-online-current-final-crx.pdf (theiia.org)

3. Developing a common understanding

3.1. The following areas are proposed for the upcoming three years, with the link back to the relevant risk(s) on the corporate risk register:

Year One (2023/4)

- Core financial controls (R73) (R46)
- Payroll (R73)
- Conflicts of interest (R73)
- Estates and facilities including sustainability (R73)
- Change and transformation programme (R88)
- International strategy (R85)

- Cyber security (R21)
- Workforce planning (R4, O4)
- Research and intelligence (R92) (R90)

Year Two (2024/5)

- Core financial controls including fee income (R73) (R46)
- Procurement and contract management (R73)
- Cyber security (R21)
- Talent management (R4) (O4)
- HR Operations including payroll (R73)
- Risk management and business continuity (R84)
- Conflicts of interest (R73)
- Stakeholder management (R72) (R90)
- Equality, diversity and inclusion (R73) (R83)

Year Three (2025/6)

- Core financial controls (R73) (R46)
- Corporate Governance (R88) (R81)
- Information management (R73)
- Guidance development (including consultation, economic impact assessment) (R92)
- FOI Casework (R26) (R90)
- Wellbeing and staff engagement (R83)
- Investigations – procedures and policies (R90) (R26)
- Cyber security (R21)

3.2. Core financial controls and cyber security are included in each year as previously recommended by our internal auditors.

4. Areas for challenge

4.1. The Committee are asked to consider the options and agree an approach to the three year annual internal audit plan.

5. Next steps

5.1. The next steps for this work is to utilise the agreed three year plan to inform discussions with our internal audit provider.

Author: Louise Byers

Consultees: Paul Arnold, Risk and Governance Board, Senior Leadership Team, Chris Braithwaite, Caroline Robinson.

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

Outcome reached: