Meeting: Audit Committee **Date:** 26 April 2021

Agenda item: 5 **Time:** 20 minutes

For discussion

Presenter: Louise Byers

Topic: Compliance at the ICO.

Issue: To provide assurance to the Audit and Risk Committee regarding the ICO's compliance with legislative requirements and identify key findings and recommendations to inform further assurance work.

Reason for report: The ICO's corporate risk register identifies compliance with legislation and other requirements as a significant corporate risk. Risk 73, Compliance Culture, sets out the '[*R]isk that as demand and capacity increase and/or changes, the ICO's infrastructure and accountability culture is unable to (Threat) keep up with the pace of change to comply with legal and other obligations expected of a modern regulator (Impact) impacting upon its ability to maintain and increase public trust and be an effective and knowledgeable regulator.'*

This risk has a gross score of (likelihood 5 x impact 4) of 20, and a current risk rating of (likelihood 4 x impact 4) of 16. In addition, the ICO has identified a number of areas relating to compliance within its Risk Appetite Statement – see Annex Two. Of particular relevance is the statement regarding organisational controls and compliance, which states:

> *"In acknowledgement of the growth and operational maturity of our multiple regulatory services, we maintain a **cautious** risk appetite towards sustaining appropriate operational processes, systems and controls to support the provision of our public services."*

Cautious is further defined as: "*Willing to accept/tolerate a degree of risk in selecting which activities to undertake to achieve key deliverables or initiatives, where we have identified scope to achieve significant reward and/or realise an opportunity; or Activities undertaken may carry a high degree of inherent risk that is deemed controllable to a large extent."* In addition to this, the appetite statements show we are, in particular,

averse to risk in relation to legal compliance, financial controls and security.

This report looks in more detail at the controls mitigating this risk and in relation to these risk appetite aeras.

Purpose of report: This paper sets out in Annex One, for the Committee's consideration, the main compliance requirements of the ICO. This is, as demonstrated below, a broad range. It includes legislative requirements that impact all businesses and organisations, such as employment law and health and safety, as well as those specific to our function as a public body, such as Freedom of Information. In addition to legislative requirements we have also identified where other documents, such as the Financial Reporting Manual, place requirements on us.

There are also many different layers of assurance for each of the requirements placed on the ICO. For ease, we have, for each of the compliance requirements, identified a first, second and third line of defence. This should give the Committee assurance that controls are in place through the 'front line' managers and teams, our internal assurance processes and teams and third-party assurance work. In terms of outcomes, many of these requirements are to produce a formal report or published statement, such as those around gender pay equality or modern slavery. Where this is the case, we have sought to indicate this.

In addition to working closely with a range of teams across the ICO, we have also had helpful input from Mazars and the ICO's legal team to identify any gaps or areas of compliance that other organisations are focussed on.

In addition to providing assurance to the Committee, it is intended that this report will also be used to identify any additional areas for review as part of the internal audit programme, as well as a programme of work for a new Compliance and Assurance role within the Risk and Governance directorate.

Background: The paper demonstrates the wide range of issues the ICO has to consider, as a public authority, an employer, a regulator, a financial institution and a data controller, amongst others.

Overall, the report shows that there is a good understanding of our compliance requirements across the organisation. However, it is also clear that there is an opportunity, through the expansion of the Risk and Governance department, to implement a more coordinated approach to compliance, and to the identification of where the law, requirements or

reporting is changing. While we have high levels of expertise across the office, we are reliant on the expertise of a broad range of individuals and teams to ensure we keep up with a fast moving and complex landscape. This report is the first step in helping to coordinate our compliance work with a dedicated compliance and assurance role forming a key part of the re-positioned Risk and Governance department. Key findings from the detailed report in Annex One include:

1) In line with our risk appetite, areas where we have an averse risk appetite, such as cyber security, are well controlled, with high levels of third party assurance and accreditation.

2) As would be expected given the reputational risk, and in line with the recent internal audit, requirements to comply with information rights law are well controlled and have a high level of oversight and assurance.

3) Where the ICO has a requirement as a regulator, for example Public Interest Disclosure, Victims Code, Safeguards Policy, National Security Certificates, Regulation of Investigatory Powers Act (RIPA) and Investigatory Powers Act (IPA) there tends to be very strong internal assurance and oversight, but more limited third party assurance. Third party involvement in compliance in these areas tends to be restricted to a right of appeal or complaint to a third party, rather than an assurance mechanism. This is also the case for our requirements for publishing certain information, where third party assurance is provided by the organisations to whom we report this information. It should be noted however that, despite the reliance on internal controls rather than third party assurance, there is very little evidence for issues being identified.

4) The opposite is true in respect of our requirements in relation to HR and Finance. The ICO's controls in these areas are heavily reliant on the first line of defence following policies and procedures and on third party assurances, given the amount of external reporting required. These areas are again included in the internal audit plan for 2021/22, which demonstrates the importance of third-party assurance.

5) It continues to be important to identify regional and national variances in compliance requirements, such as the Welsh language scheme and the additional equality reporting duties in Northern Ireland.

Key recommendations resulting from this work include that:

1) This report should be updated and brought to the Risk and Governance Board and Audit Committee each year.
2) This report forms the basis of the development of training and communication to our managers about their compliance responsibilities.
3) Work should be undertaken to clarify and strengthen the role and oversight and assurance mechanisms in place in our second line of defence teams, for example HR, Finance and Procurement. This work should be overseen by the Risk and Governance Board and a programme of compliance assurance developed.
4) Where we have a reporting duty, we should continue to ensure that this information is made available to staff and external advisors, such as on equality and diversity and gender pay reporting.
5) Through our ongoing work on scorecards and KPIs, we should identify risk indicators that show changes in compliance – including performance in key compliance processes such as finance, HR, and complaints and request handling, and information management, cyber and security. These could then be used for form a 'compliance' dashboard.
6) Risk 73 should be reviewed and broadened to a wider compliance risk. This would decouple the risk from changes in demand and make clear that both the internal and external environment drives compliance risk at the ICO. Suggested wording is below:

'[*R]isk that as the organisation grows, and/or the external compliance requirements change, the ICO's infrastructure and accountability culture is unable to (Threat) keep up with the pace of change to comply with legal and other obligations expected of a modern regulator (Impact) impacting upon its ability to maintain and increase public trust and be an effective and knowledgeable regulator.'*

Next steps: In discussing the report, we would like the Committee to consider:

- Are there any gaps in this compliance requirements and/or controls identified?
- Are the any areas where the controls identified are not proportionate to the risk – in particular where we do not have enough oversight and assurance?

- Are there any areas where the Committee would benefit from additional third-party assurance as part of the 2021/22 Internal Audit plan?
- Does Risk 73 adequately cover the ICO's compliance risk?

Resource implications: The resources implications are primarily in relation to ensuring the internal audit plan is focussed on the right areas of compliance risk and that a clear work programme is developed for a compliance and assurance role within the Risk and Governance department.

Equality, diversity and inclusion considerations: There are no specific EDI considerations, however EDI reporting across the UK forms a key part of our compliance requirements.

Alignment with values: Ensuring the ICO continues to comply with its requirements as a public body, business, employer, regulator and data controller will enable us to continue to deliver on the values of ambition, service focus and collaboration.

Impact on Risks and Opportunity Register: As set out in the report, the paper is most relevant to Risk 73, Compliance Culture, currently described as the '[*R]isk that as demand and capacity increase and/or changes, the ICO's infrastructure and accountability culture is unable to (Threat) keep up with the pace of change to comply with legal and other obligations expected of a modern regulator (Impact) impacting upon its ability to maintain and increase public trust and be an effective and knowledgeable regulator.'*

Publication considerations: This report is not considered suitable for external publication but can be published internally.

Author: Louise Byers

Consultees: SLT, Heads of Department, Risk and Governance Board

List of Annexes:

Annex One – ICO Compliance – Detailed Review

Annex Two – Risk Appetite Statement