Risk Management Policy and Appetite Statement

Document name	Risk Management Policy and Appetite Statement
Version number	4.4
Status	Published
Department/Team	Planning, Risk & Governance
Relevant policies	Risk & Opportunity Management Procedure
Distribution	Internal and External
Author/Owner	Joanne Butler
Approved by	Risk Management Policy: Audit & Risk Committee Risk Appetite Statement: Management Board
Date of sign off	15/5/23
Review by	31/1/24
Security classification	Official

Key messages

The main objective of this policy is to:

- Form part of the Information Commissioner's Office's (ICO) internal control and corporate governance arrangements.
- Clearly outline the ICO's commitment to risk management
- Describe the goals and objectives of risk management
- Provide a framework for continuing to embed risk management across the organisation
- Set the tone for the organisation and increases the likelihood that the management of risk will be given appropriate consideration by all.

Does this policy relate to me?

Risk Management must be embedded into the ICO's culture and all of its activities, as such, all staff have a role to play to ensure the ICO's risk management framework is effective and should familiarise themselves with the policy.

Table of contents

1. Risk Management Executive Summary

1.1. This risk management policy and appetite statement forms part of the Information Commissioner's Office's (ICO's) internal control and corporate governance arrangements. This policy, and the adoption of the overall risk management framework, including allocating proportionate resources to risk management, is owned by the Chief Operating Officer. Risk Management must be embedded into the ICO's culture and all of its activities, as such, all staff have a role to play to ensure the ICO's risk management framework is effective. A summary of roles and responsibilities in relation to risk management is detailed in the ICO's Risk and Opportunity Management Procedure.

1.2. The purpose of this policy is to clearly outline the ICO's commitment to risk management, describe the goals and objectives of risk management, and provide a framework for continuing to embed risk management across the organisation, with defined roles and responsibilities and a structured process. It sets out the commitment from the Commissioner and ICO senior managers to managing risks effectively across the ICO, and the standard of risk management we deliver across the ICO. It sets the tone for the organisation and increases the likelihood that the management of risk will be given appropriate consideration by all.

1.3. As the ICO looks forwards, even in a short period of time there will be a host of factors which influence the nature of the ICO's regulation duties and the environment in which it operates. These factors challenge the ICO to continually review its systems and approaches, and to experiment with new ideas allowing mixed and flexible use of resources. The Commissioner and ICO senior managers and decision makers, will all face existing, new and evolving risks to achieving the ICO's objectives. This will be against a backdrop of a constantly evolving environment, with a need to continually adapt internal organisation and shifts of approach to meet technological and social changes, new legal requirements and economic challenges.

1.4. Our four core values: curious, collaborative, impactful and respect, equality, diversity and inclusivity are central to risk management. They influence our risk culture, the way we plan, make decisions, how we behave towards one another and continually challenge ourselves to achieve our vision and impact.

1.5. Effective risk management is not about avoiding all risk: with an effective risk management culture and strengthened understanding of risk management we may decide to take more risks in some areas of the organisation. This will always be on an informed basis, ensuring that the benefits of the risk-taking enable us to achieve our ambitions and help us to innovate as effectively and cost efficiently as possible, as we continue to achieve the goals of our ICO25 corporate plan, enduring objectives and underpinning strategies.

1.6. Through the implementation and embedding of an effective risk management framework, and the setting of an appropriate risk appetite, we will ensure that we are ideally placed to achieve our objectives by providing regulatory certainty and deliver impactful regulatory outcomes.

Back to Top

2. Introduction

2.1 A risk is an expression of uncertainty to achieving objectives and can be a threat or an opportunity. A threat is a possible future event or action which will adversely affect the ICO's ability to achieve its goals, priorities and objectives and to successfully deliver approved strategies. An opportunity is an event or action that will enhance the ICO's ability to achieve its goals, priorities and objectives and deliver approved strategies. Risk is part of everything we do. Managing risk improves the way we deliver our services. It is acknowledged that some risks will always exist and will never be eliminated, but through risk identification we anticipate eventualities and it helps us to respond to changes in need and to prepare response plans where we can. This ensures that we can minimise/maximise the likelihood of a risk occurring as far as possible, or minimise/maximise the impact if it does happen.

2.2. The ICO will manage risk (both threats and opportunity), effectively and in a consistent manner in all aspects of its business including planning, delivering, operating and overseeing programmes and performance. All management levels will develop and encourage a culture of well-informed risk-based decision making. Managing risk will be at the core of the ICO's governance, enabling sound strategic and operational decision making and good business management. Risks are focused on how they affect our ability to deliver objectives. To enable this, we hold risk registers at various levels, such as: a corporate risk register for risks which affect our ability to achieve corporate objectives; Directorate risk registers for risks which affect our ability to achieve Directorate objectives; and project risk registers, for risks which affect our ability to achieve the objectives of the specific project

2.3 There are 4 goals detailed below which outline the ICO's approach to risk management and internal control.

Back to Top

3. Goal #1: Risk Governance

Risk management will be embedded into the ethos, culture, policies and practices of the ICO so that risk management is an integral part of decision making, management and governance practices.

3.1 Considering and responding to existing and new threats, and the ability to recognise and seize new opportunities, is fundamental to achieving the ICO's desired goals and key strategic priorities. Underlying this is a commitment from the ICO to promote openness, transparency and accountability and good governance. Decisions made by the ICO are evidence-based and subject to appropriate challenge. This requires high standards of corporate governance. Effective risk management is a key principle of corporate governance and a key contributor to a sound control environment.

3.2 Risk management plays a key role in helping us achieve our enduring objectives and priorities. It helps ensure decision-making is better informed, ensures public resources are used efficiently and helps us to avoid unwelcome surprises.

3.3 The following actions will help us to achieve Goal#1:-

Action: We will ensure the effectiveness of the ICO's risk management framework, so that the Commissioner, Management Board and ICO senior management are able to rely on adequate three lines of defence functions. This includes monitoring and assurance functions undertaken by the Audit and Risk Committee and the Risk and Governance Board.

Action: We will ensure that good risk management is an integral part of everyday governance business, including policy making, decision making, performance management, business planning, prioritisation and assurance activity.

Action: We will ensure that internal audit coverage is driven by a clear understanding of the risks, challenges and opportunities facing the ICO. Some of the risks will be unique to individual service areas and functions within the ICO; others will be common to other regulators and organisations, giving opportunities for benchmarking.

Back to Top

4. Goal #2: Risk Culture

We will ensure we have an organisational culture which empowers staff to undertake well managed risk-taking and are able to escalate risks and concerns

4.1 A strong risk culture is one that expresses its values and defines expected behaviours. Staff understand how cultural attributes are measured and its values are aligned with reward processes.

4.2 The following actions will help us to achieve Goal#2:-

Action: ICO senior management will lead by example with a combination of positive attitudes, behaviours and activities to create an environment where curiosity and consideration of risk is part of everything we do.

Action: ICO senior managers will lead by example by taking ownership and being transparent and accountable for Corporate and Directorate level risks, ensuring that effective and proportionate action is taken to mitigate those risks so that we can achieve our objectives

Action: We will encourage service excellence and innovation, taking considered risks; and, engender a continuous improvement mind-set towards the way we manage risk, and implement learning lessons, and in doing so, improve delivery of our regulatory services.

Action: We will promote open, honest and collaborative discussions about our risks. We will ensure we understand all perspectives and encourage inclusion and a no-blame risk environment and culture.

Action: We will communicate clear messages, ensuring everyone understands the role they have to play in identifying and managing the risks and opportunities we face in the successful delivery of our strategic plans, projects, and day to day service delivery business objectives.

Action: We will ensure our risk work makes a material difference escalating risks to ensure they are managed effectively and with impact.

Back to Top

5. Goal #3: Risk Skills

We will ensure that staff have the skills and knowledge they need to fulfil their risk management responsibilities

5.1 Educating staff is particularly important in risk management to have an effective risk framework in place. The greatest risks tend to be related to people and our people are also our greatest control mechanism. This includes understanding of the organisational risk appetite, as well as risk management practices.

5.2 The following actions will help us to achieve Goal#3:-

Action: We will equip ICO staff with the tools, skills and time they need to fulfil their risk management responsibilities. This will include the provision of training, guidance, templates, and by allowing time on meeting agendas for risk discussion.

Action: We will encourage and support staff in identifying and discussing risk in their everyday business; and to pro-actively deal with risks that come to their attention.

Action: We will provide opportunities for shared learning on risk management across the ICO and with other regulators, partners and stakeholders where appropriate.

Action: We will encourage a network of risk champions to help raise awareness and understanding of risk management at all levels across the business.

Back to Top

6. Goal #4: Risk Management Approach

The ICO will successfully manage risk and opportunities at all levels – strategic, operational, programme, project and in collaboration activity, so that is increases the probability of achieving its goals and priorities

6.1 Accountability for service delivery brings with it responsibility for identifying, assessing, owning, managing and communicating key risks to service delivery. This requires the collaborative effort of our management, all our staff and any key partners.

6.2 The following actions will help us to achieve Goal#4:-

Action: We will adopt a consistent application and embed an agreed business risk management approach throughout the ICO establishing a risk and opportunity management procedure which clearly defines the roles, responsibilities and reporting lines within the ICO for risk management.

Action: We will integrate the management of risk into all of our business processes, including (but not limited to) regulatory, finance, planning, performance management, prioritisation, key decision-making processes, portfolio, programme and project management and major change initiatives.

Action: We will maintain a hierarchy of risk registers, that are regularly reviewed and monitored to ensure that key risks are visible, are owned at the right level of the organisation, and are actively addressed. We will ensure that risks are escalated or de-escalated appropriately between the risk registers, and will ensure that cross-cutting risks identified in multiple registers are appropriately managed. Where appropriate we will identify and monitor risk indicators for significant risks

Action: We will use national and best practice guidelines on risk management and risk maturity. We will engage in relevant risk management forums and benchmarking exercises to identify further opportunities for improvement in our approach to risk management.

Back to Top

7. Internal Control and Risk Management

7.1 The system of internal control incorporates risk management. This system encompasses a number of elements that together facilitate an effective and efficient operation, enabling the ICO to respond to a variety of operational risks.

7.2 These elements include:

a. Policies and procedures: Attached to significant risks are a series of policies that underpin the internal control process. The policies are approved and implemented and communicated by senior management to staff. Written procedures support the policies where appropriate.

b. **Planning and Performance Management:** By integrating risk management with the ICO's strategic, regulatory and financial planning, budgeting and performance management processes and individual service and business delivery plans we are able to monitor risks to achieving the objectives, determine which risks have the most significant impact, recognise where risks are increasing or decreasing and prioritise resource accordingly.

c. **Prioritisation:** We will take account of risk as part of our prioritisation processes for delivery of activity across the business ensuring that risks are recognised and managed in order to achieve our shifts of approach and ICO25 enduring objectives.

d. **Horizon Scanning:** This approach to risk management informs the ICO's business processes, and includes regular risk horizon scanning through strategic planning, including the strategic threat assessment and work of the intelligence team; service and business planning and performance, policy making and review work undertaken by the Regulatory Futures Directorate, as a core part of their business area. Horizon scanning for risks is also undertaken through our programme and project work and through partnership working and collaboration with other regulators and public bodies. We also make good use of our networking arrangements and relationship with both our internal and external auditors to stay alert to new and emerging risks

e. **Reporting and Annual Report:** Comprehensive review and reporting is designed to monitor key risks and their controls. Decisions to rectify problems are made at regular meetings of the Executive Leadership Team. The Audit and Risk Committee's Annual Report includes a review of the effectiveness of the internal control system. The Risk and Governance Board reviews corporate risks at every meeting.

f. **Strategic Threat Assessment (STA):** The STA aims to support ICO decision-makers to prioritise and direct our resources, relationships and regulatory effort. The STA also aims to assist staff to identify and share actionable intelligence across the organisation and externally.

g. **Information Risk & Governance Group:** The Information Risk & Governance Group (IRGG) is responsible for the overview and scrutiny of information governance (IG) arrangements and for making recommendations to the Risk and Governance Board and the Senior Information Risk Owner (SIRO) on information governance decisions.

The Group provides assurance that; an effective and efficient IG framework is in place, that the ICO is compliant with regulations; and that information governance risk is well managed across the organisation.

h. Business Continuity: The business continuity process is essentially risk management applied to the whole organisation and its ability to continue with its service provision in the event of a catastrophic event. The ICO has developed a complimentary Business Continuity Policy to Risk Management alongside its corporate Business Continuity Plan.

i. Anti-Fraud: The ICO has a fraud response plan, which directs staff towards ensuring a professional and ethical approach to combating fraud.

j. Whistleblowing: The ICO is committed to the highest possible standards of openness, probity and accountability. Employees, contractors, suppliers to or consultants with, the ICO are often the first to realise that something wrong may be happening within. "Speak up", the ICO's Whistleblowing Policy and Procedure is intended to help those who have concerns over any potential wrong-doing within the ICO.

k. Audit and Accreditation reports: The ICO makes reference to and acts upon the results of the work of the internal and external auditors and on information and recommendations received from other feedback mechanisms, including governments, professional bodies and accreditation bodies.

Back to Top

8. Information Commissioner's Office Risk Appetite Statement

8.1 This risk appetite statement sets out how the ICO balances threats and opportunities in pursuit of achieving its objectives. Understanding and setting a clear risk appetite level is essential to achieving an effective risk management framework. In addition, establishing and articulating the risk appetite levels helps to ensure that the ICO responds to risk consistently, in line with a shared vision for managing risk and helps us to form a positive organisational culture by providing the guidelines for managing risk so that we can make changes to best effect. A sound risk management culture helps us to inspire high performance, allows us to discuss ideas for new initiatives and decide on the best approach to solving a problem.

8.2 Public sector organisations cannot be risk averse and be successful. There are risks facing the ICO such as legal compliance where its risk appetite may be very low. Conversely there are risks with choices about change and development, projects, research and delivery roles, where some risk taking is expected. The risk appetite sets out the level of residual risk which is tolerable: where the risk appetite is low, we will either choose options which have low risk, or devote more resources into making sure that we have fully mitigated the risks of the option we want to pursue; where the risk appetite is high, we are more likely to choose options with a high degree of risk or devote less resources to mitigating the risks.

8.3 The risk appetite statement forms a key element of the ICO's assurance and governance framework and is set by the Commissioner and their Management Board. There may be instances where the ICO chooses to tolerate an increased level of risk above the risk appetite, in this case the decision to do so will be escalated and authorised. Breaches of risk appetite, or tensions arising from its implementation will be dealt with by the Executive Team and may reflect a need to review the risk appetite statement.

8.4 In determining the statement it is recognised that risk appetite is subject to change and needs to flex in line with the organisation's strategic environment and business conditions; and as such the statement will be reviewed on a regular basis and at least annually.

8.5 The ICO distinguishes between those risks which are mostly operational in nature (and as such are within our control) and those external risk factors which are not directly within our control but which nevertheless must be identified and considered to address those risks we can influence or contingency plans we need to make. This will be discussed and escalated through internal line management chains.

Back to Top

9. Context to the Risk Appetite Statement

9.1 The ICO does not have a single risk appetite, but rather appetites across the range of its activities. The ICO recognises that in pursuit of its ICO25 enduring objectives, strategic priorities and outcomes that it may choose to accept different degrees of risk in different areas. For example, we may be prepared to take greater risk in our regulatory work but be more risk averse in financial matters.

9.2 The ICO has established and articulated its risk appetite for differing areas where it is beneficial to ensure consistency in our approach to managing risks, and to empower decision makers to take appropriate decisions about risk.

Back to Top

10. Risk Appetite Definitions

10.1 The parameters for appraisal of risk are summarised within the risk appetite definitions as follows:-

Appetite	Rank	Description
Hungry	5/5	We are eager to be innovative and will proactively take creative and pioneering delivery approaches to help maximise opportunities whilst accepting the associated substantial risk levels in order to secure highly successful outcomes and benefits
Open	4/5	We are prepared to consider a number of potential delivery approaches, even where there are elevated levels of associated risk, and will choose the option which provides a high probability of productive outcomes and benefits.
Cautious	3/5	We are willing to accept modest and largely controllable levels of risk in order to achieve acceptable key, but possibly unambitious, outcomes or benefits.
Minimalist	2/5	We have an overall preference for safe delivery approaches and whilst we are willing to accept some low level risks, the potential for increased outcomes and benefits is not the key driver.
Averse	1/5	We will take very safe delivery approaches and accept only the very lowest levels of risk, avoiding risk and uncertainty as a key objective, whilst recognising that this may restrict exploitation of opportunities and innovation.

Back to Top

11. Risk Appetite Levels

11.1 The ICO's risk appetites cover a range of activities and are linked to the ICO25 objectives and shifts of approach. The risk appetite statements help empower staff to make appropriate decisions about risk taking in their role. The statements also enable a shift in organisational culture so that staff are comfortable in taking risks within appetite and make decisions without the need to escalate. Risk appetite will be considered as part of our prioritisation techniques through our shifts of approach.

11.2 As described above, the risk appetite is the broad description of the amount of risk the ICO is willing to accept or retain in order to achieve its objectives. It is a statement or series of statements that describe the organisation's attitude towards risk taking.

The ICO has articulated our risk appetite for ambiguous areas of risk where a clear statement will help staff to understand how much risk we are willing to take, to guide their decisions, and indicates what needs to be escalated and the choices we are making.

People:

- Recruitment: We have a ***hungry*** appetite (*are willing to take significant risks*) when it comes to recruitment, using creative and pioneering ways of finding and attracting new talent.
- Wellbeing: We maintain a ***minimalist*** risk appetite (*are willing to accept some low level risks*) for risks impacting on staff wellbeing and the ICO will continually focus on balancing both organisation and employee needs.
- EDI: We have an ***open*** risk appetite (*willing to accept elevated levels of risk*) to innovative ways of working that enable us to be an inclusive employer and regulator.
- Empowering: We have an ***open*** risk appetite (*willing to accept elevated levels of risk*) to supporting and empowering our staff to perform in their role.
- Behaviour: We have a ***minimalist*** appetite (*are willing to accept some low level risks*) to conduct and behaviours that are not in line with our values and our equality, diversity and inclusion objectives.

Data, Digital and Information:

- Transparency: We take an ***open*** approach (are *willing to accept elevated levels of risk*) when considering the transparency of our work and will look to be transparent wherever possible, even if there are associated risks.
- Digital Delivery: We have a ***hungry*** approach (*are willing to take significant risks*) in how we provide digital delivery methods and will maximise our use of technology, even where there is some associated risk, if there is the potential for better outcomes for our people and stakeholders.
- Security: In taking the two above approaches to risk appetite we also need to balance accepted risks with maintaining a ***minimalist*** risk appetite (*are willing to accept some low level risks*) to the security of our data, especially in relation to information and cyber security, and we will put in place robust processes to ensure we proportionately mitigate the risk.

Compliance & Resources:

- Compliance: We have an ***averse*** risk appetite (*are unwilling to accept risk*) non-compliance with ICO policies where they have a 'must' requirement to do (or not do) something.
- Policies and Procedures: We maintain a ***minimalist*** risk appetite (*are willing to accept some low level risks*) for areas of ambiguity in applying our policies and procedures when an element of judgment is required.
- Financial Planning: We have a ***cautious*** risk appetite (*are willing to accept controllable levels of risk)* in our financial planning and, as a responsible public sector organisation, we may prefer to choose the safe options that have a low degree of inherent risk.
- Resource: We have a ***hungry*** risk appetite (*are willing to accept significant risks*) to discontinuing work where there is no evidence of significant harm, or where it does not contribute to achievement of our objectives.

Regulatory:

- Certainty: We maintain a ***hungry*** appetite (*are willing to accept significant risk*) to using new ways of providing organisations with the certainty they need to do their work and for members of the public to use their rights.

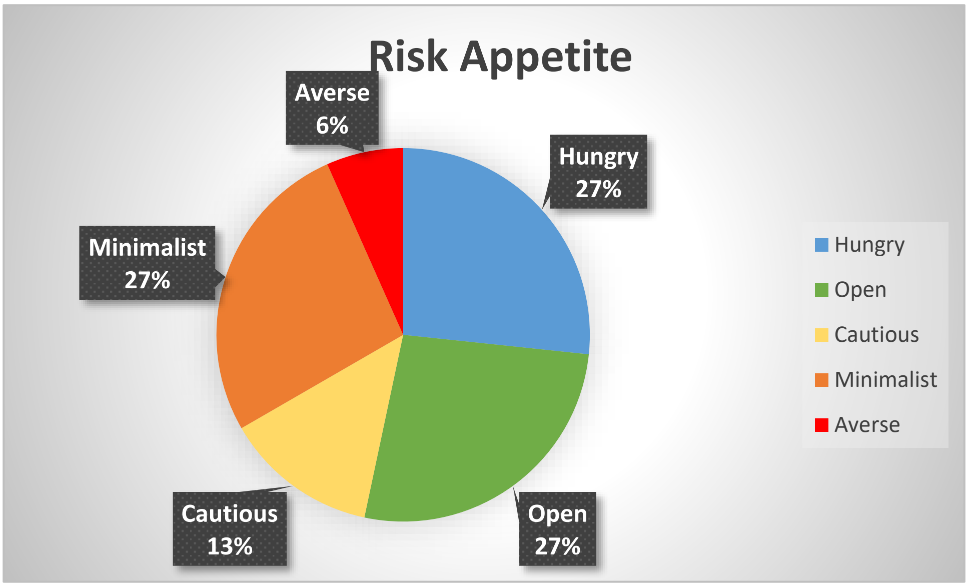
- Prevention: We are ***open*** (*are willing to accept elevated levels of risk*) to intervening to prevent future harms, and to use our powers where they are needed.
- Legal: In taking the two above approaches to risk appetite we also need to balance accepted risks with maintaining a ***cautious*** appetite (*are willing to accept controllable levels of risk)* to behaving in an unlawful or irrational way.

Back to Top

12. Risk Appetite Tables

Hungry	We will proactively take creative and pioneering decisions and delivery approaches while accepting the associated substantial risk levels in order to secure highly successful outcomes and benefits	✓ Recruitment ✓ Resource ✓ Certainty ✓ Digital Delivery
Open	We are prepared to consider innovative decisions and delivery approaches, even where there are elevated levels of associated risk, if there is a high probability of productive outcomes and benefits.	✓ Empowering ✓ Transparency ✓ Prevention ✓ EDI
Cautious	We are willing to accept modest and largely controllable levels of risk in order to achieve acceptable key, but possibility unambitious, outcomes or benefits.	✓ Financial Planning ✓ Legal
Minimalist	We have an overall preference for safe decision making and delivery approaches but are willing to accept some low level risks, despite the probability that there is restricted potential for innovation and increased outcomes and benefits.	✓ Wellbeing ✓ Behaviour ✓ Security ✓ Policies & Procedures
Averse	We will take very safe decision making and delivery approaches and accept only the very lowest levels of risk, avoiding risk and uncertainty where we are able, whilst recognising that this may restrict exploitation of opportunities and innovation.	✓ Compliance

13. Risk Appetite Heat Map



[Back to Top]

14. Risk Capacity

13.1 The ICO's risk capacity is determined through understanding its risk environment. This includes whether the ICO can withstand reputation pressures as a result of the activity; if there is sufficient financial contingency; what political tolerance there is for any adverse risk events materialising, both internally and externally; what pressures the activity places on the ICO's regulatory position; if there is sufficient infrastructure and sufficient capacity and capability to manage risk; or if it is an area of priority.

[Back to Top]

Feedback on this document

If you have any feedback on this document, please click this link to provide it.

[Back to Top]

Version history

Version	Changes made	Date	Made by
4.3	Transferred to a new template.	10/11/2022	Caroline Robinson
4.4	Risk Appetite Statement reviewed and updated in line with ICO25	25/5/23	Caroline Robinson

Back to Top