Risk Management Policy and Appetite Statement

Version number: 4.6

Status: Draft

Department/Team: Risk & Governance

Relevant policies: Risk & Opportunity Management Procedure

Distribution: Internal and External

Author/Owner: Joanne Butler

Consultees: Executive Team, Risk Champions

Approved by: Management Board

Application date: 31/3/25

Review date: 31/3/26

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 and approach to risk management
- Describe our goals and objectives for risk management
- Provide a framework for continuing to embed effective and proportionate risk management across the organisation
- Set the tone and ethos for the organisation
- Ensure that the value of effectively managing risk is understood by all.

Does this policy relate to me?

All staff should familiarise themselves with our risk management policy and risk appetite statement as we all need to know how to manage risk and what this means in our day-to-day work. It helps us to decide how to handle a threat or an

opportunity so that we can make good decisions, and know how best to prioritise our actions so that we are better placed to achieve our objectives.

The risk appetite statements within the policy help to guide and coordinate our decisions so that we are all taking the same level of risk across the organisation.

Management Board have set the risk appetite levels so that we are empowered to take decisions about risk as close to the activity as possible.

Table of contents

1. Foreword[1]

Welcome to the Risk Management Policy and Appetite Statement for the Information Commissioner's Office (ICO). At the ICO we believe in the

[1] *Orange Book (OB):A7/A10*

value of effectively managing risk: it informs business decisions; enables a more effective use of public resources; enhances strategic and business planning; and strengthens contingency planning.

Taking appropriate and effectively managing and mitigating risks is essential to the work of the ICO. It is how we experiment and innovate and ensure our work is able to remain relevant and keep pace with the world we regulate and operate in as an employer. We must also avoid taking, or failing to mitigate risks, which might lead to outcomes or negative impacts we consider to be intolerable or unacceptable.

Having a shared understanding of our collective appetite and tolerance for the different risks and opportunities across the work of the ICO is therefore integral to being an efficient, productive and well run organisation.

With this in mind, the ICO continues to develop a risk ethos that focuses on assessing, managing and monitoring risks. As we continue to mature our risk culture and approach to risk management, this policy and appetite statement ensures that Risk Management is at the centre of what we do.

This policy applies to all who work at the ICO. It empowers us to seek strategic opportunities, whilst recognising that innovation and good governance are not mutually exclusive. It supports us to get the foundations of effective risk management right and to do so together as one ICO.

Paul Arnold MBE
Deputy Chief Executive and Chief Operating Officer.

2. Risk Management Executive Summary

2.1 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[2] to risk management, is owned by the Executive Director, Strategy & Resources[3].Risk Management must be

[2] *OB:A9*
[3] *OB:A8*

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[4] in relation to risk management is detailed in the ICO's Risk and Opportunity Management Procedure.

2.2 The purpose of this policy is to clearly outline the ICO's commitment to risk management, describe the goals and objectives , and provide a risk framework for continuing to embed risk management across the organisation., It sets out the commitment from the Commissioner and senior managers to managing risks effectively., It sets the tone for the organisation, helps promote good risk taking through influencing the risk culture and increases the likelihood that the management of risk will be given appropriate consideration by all.

2.3 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 be innovative allowing mixed and flexible use of resources. Our decision makers all face existing, new and evolving risks to achieving the ICO's objectives. This will be against a backdrop of a constantly evolving environment, alongside a need to continually adapt our internal organisation and shifts of approach to do it differently to meet technological and social changes, new legal requirements and economic challenges.

2.4 Our four core values: curious, collaborative, impactful and inclusive are central to risk management. They influence our risk ethos, the way we plan, make decisions, how we behave and how we continually challenge ourselves to achieve our vision and impact.

2.5 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

[4] *OB:A4*

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.

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

Back to Top

3. Introduction

3.1 Risks can be considered simply as "uncertainties that matter". A risk is a possible future event that will either adversely or beneficially affect our ability to achieve our objectives. It considers both sides of the risk coin, ie., threats and opportunities:-

- A threat is a possible future event or action which will adversely affect the ICO's ability to successfully achieve its goals, priorities and objectives.
- An opportunity is an event or action that will enhance our ability to achieve these.

Risk is part of everything we do. Managing risk improves the way we deliver our services. Some risks will always exist and will never be eliminated, but through our risk identification we can anticipate and respond to risks where we can. This means that we are better able to:-

- minimise the likelihood and impact of a threat occurring to within our risk appetite, or
- maximise the likelihood and impact of an opportunity happening to help us achieve our objectives.

3.2. 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 portfolio, programme and project risk registers, for risks which affect our ability to achieve the objectives of specific projects[5].

3.3 We have 4 goals detailed below which outline the ICO's approach to risk management and internal control.

Back to Top

4. Goal #1: Risk Governance & Leadership[6]

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 at all levels.

4.1 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.

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

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

[5] *OB:A3*

[6] *OB:Principles A & B*

Action[7]: We will ensure the effectiveness of the ICO's risk management framework, so that the Commissioner, Management Board and Audit and Risk Committee are able to rely on an adequate three lines model of control. This includes monitoring and assurance functions undertaken by management in the first and second line roles, and an independent third line role from internal audit.

Action[8]: We will ensure that the Commissioner and Management Board receive a balanced assessment of the ICO's corporate risks and the effectiveness of risk management, including how those risks will be managed within plans. Senior leaders will ensure that the quality of risk information provided is sufficient to allow effective decision making.

Action[9]: 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. Risks will be transparent and considered against our risk appetite as part of appraising and evaluating options and making informed decisions.

Action[10]: 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

5. Goal #2: Risk Ethos [11]

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

5.1 An organisation with a strong risk ethos is one that expresses its values and defines expected behaviours. Staff understand how culture and behaviours are measured and how ICO values are aligned with our

[7] *OB:A4*
[8] *OB: A6/B3*
[9] *OB: A5/B1/B2*
[10] *OB:A4/C4*
[11] OB:A1/A2

reward processes. Our risk ethos, risk appetite and values guide our actions and decisions.

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

Action[12]: ICO senior management will lead by example through a combination of positive attitudes and behaviours. They will encourage feedback, create an environment where curiosity and consideration of risk is second nature.

Action[13]: ICO senior managers will lead by example by taking ownership and being transparent and accountable for Corporate and Directorate level risks. we will demonstrate recognition of our risk appetite and ensure that effective and proportionate action is taken to manage risk.

Action[14]: We will encourage staff to feel more invested in the success of our risk management policy by giving them a sense of ownership and empowerment to risk taking.

Action[15]: We will promote curious, open and collaborative discussions about our risks. We will ensure we understand all perspectives, encourage inclusion and seek a no-blame risk culture.

Action[16]: 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, programmes, projects, and day to day work. .

Action[17]: We will ensure our risk work makes a material difference escalating risks to ensure they are managed effectively, proportionately, in line with our risk appetite and with impact.

Action[18]: We will undertake an annual risk maturity culture assessment and have regular conversations with our people to understand risk motivation and satisfaction so that we may work together to strengthen risk culture.

---

12 *OB:A10*
13 *OB:A4/A10*
14 *OB:A1/A4/A5*
15 *OB:A1/A4/A5*
16 *OB:A4/A5*
17 *OB:A5*
18 *OB:A6*

Action[19]: We will recognise that creating a strong risk ethos is a gradual process so we will be patient and persistent. We will continually communicate how risk management helps us to achieve our organisational plans, how we all own risks, and consistently demonstrate. the above actions.

6. Goal #3: Risk Skills

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

6.1 Some of our significant risks are related to people, and our people also provide our best mitigation. Ensuring we educate our staff about risk management is really important. This includes understanding the ICO's risk appetite, as well as risk management practices.

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

Action[20]: 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 encouraging time on meeting agendas for risk discussion. Our risk management guidance, tools and training will be kept up to date.

Action[21]: We will encourage staff to identify and discuss risk in their everyday business. We will support them to pro-actively deal with risks that come to their attention and to know when to escalate a risk.. We will encourage lessons learned to be captured, evaluated and action taken.

Action[22]: We will provide opportunities for shared learning on risk management and lessons learned to assist with risk management in the future. We will encourage learning from previous experience both across the ICO and with other regulators, partners and stakeholders where this is appropriate.

---

19 *OB:A1/A5/A7/A10*
20 *OB:C4/C5/C6/E2/E4*
21 *OB:C1/E2*
22 *OB:C1/C2/C3/C4/C5/E2*

Action[23]: We will improve our risk maturity by encouraging and supporting a network of risk champions to help coordinate our risk practices. They will help to raise awareness and understanding of risk management at all levels across the business.

Back to Top

7. Goal #4: Risk Management Approach[24]

The ICO will manage risk and opportunities at all levels of its objectives, including cross-functional objectives and collaborative activity, so that we increase the probability of success. Risk Management will be collaborative and informed by the best available information and expertise.

7.1 Accountability for service delivery brings with it responsibility for identifying, assessing, owning, managing and communicating key risks to service delivery. This requires collaborative effort from managers, staff and any key partners.

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

Action[25]: We will embed a consistent risk management approach throughout the ICO establishing a risk and opportunity management procedure which clearly defines the roles, responsibilities and reporting lines for risk management.

Action[26]: 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[27]: We will maintain a hierarchy of risk registers, that are regularly reviewed and monitored to ensure that key risks are visible, owned at the right level of the organisation, and are actively addressed. We will ensure that risks are escalated or de-escalated appropriately.

---

23 *OB:C4/C5/C6*
24 *OB:A4/A5/Principle C*
25 *OB:A4/A5*
26 *OB:A5/C6*
27 *OB:A5/C1/C5/C6*

Where appropriate we will identify and monitor risk indicators for significant risks and ensure that cross-cutting risks are appropriately managed.

Action[28]: 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.

Action[29]: We will horizon scan and take account of other relevant risk register information such as the National Risk Register and partnership risks with our key partners and sponsoring body where these risks may impact on the achievement of our objectives.

Back to Top

8. Internal Control and Risk Management

8.1 The ICO's internal control includes good risk management. This includes a number of elements which enable the ICO to respond to a variety of risks.

8.2 These elements include:

a. **Policies and procedures[30]:** 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[31]:** By integrating risk management with the ICO's strategic, regulatory and financial planning, budgeting and performance management processes, we are able to monitor risks to achieving our objectives. This helps us to determine which risks have the most significant impact, recognise where risks are increasing or decreasing and prioritise our resource accordingly.

c. **Prioritisation[32]:** Our prioritisation tool and framework, which is to be applied across all the ICO's activities ensures that risks to protecting the public, delivery and reputation are identified at the earliest

[28] *OB:A10/E1/E2/E3/E4*
[29] *OB:B4/C2/C4*
[30] *OB:A2*
[31] *OB:A5*
[32] *OB:A5/B5/C3*

opportunity before committing to undertaking work in order to achieve our objectives.

d. Horizon Scanning[33]: This approach to risk management informs the ICO's business processes, and includes regular risk horizon scanning. This includes the work of strategic planning and intelligence,; and policy making. 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 relationships with both our internal and external auditors to stay alert to new and emerging risks.

e. Reporting and Annual Report[34]: The Annual Report and Financial Statements includes information of the risk assessment and risk management over the previous year, along with the internal auditor's assessment of the overall internal control framework, of which risk management is a key part. In addition, the Audit and Risk Committee produces its own Annual Report which gives a view of the successful operation of the internal control framework.

f. Information Risk & Governance Group[35]: 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.

g. Business Continuity[36]: 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 critical incident or catastrophic event. The ICO has developed a complimentary Business Continuity Policy to Risk Management alongside its corporate Business Continuity Plan.

---

33 *OB:A5/B4*
34 *OB:A6*
35 *OB:A5*
36 *OB:A5*

h. Anti-Fraud[37]: The ICO has a Counter Fraud, Bribery and Corruption policy and procedure to reduce the risk of fraud and highlights controls to deter, prevent and identify fraud. Senior management ensure that appropriate risk assessments are conducted in relation to fraud, bribery and corruption and that the control framework is robust.

i. Whistleblowing[38]: 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.

j. Audit and Accreditation reports[39]: 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.

k. Health and Safety: The Estates and Facilities department is responsible for ensuring the ICO is compliant with Health and Safety legislation and implements good practice to minimise risk to our staff and visitors. There are a wide range of policies and safety processes in place to support delivery of this objective, with activity being overseen by the Health, Safety and Wellbeing Committee which is able to escalate matters to relevant boards.

Back to Top

9. Information Commissioner's Office Risk Appetite Statement

9.1 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

[37] *OB:A2/A5/C3*
[38] *OB:A2/A5*
[39] *OB:A4*

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.

9.2 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.

9.3 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[40]. 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.

9.4 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.

9.5 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.

[40] *OB:A3*

Back to Top

10. Context to the Risk Appetite Statement

10.1 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.

10.2 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. Our risk appetite statements aid our decision-making across the organisation and are not just a tool for managing our corporate risks, decisions should take account of what the residual risk will be following a proportionate and achievable response to the risk.

10.3 Where applicable we have aligned our risk appetite areas with the risk appetite example categories within the Orange Book Risk Appetite Guidance Note.

Back to Top

11. Risk Appetite Definitions

11.1 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

Appetite	Rank	Description
		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

12. Risk Appetite Levels

12.1 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 and through our shifts of approach and doing it differently work.

12.2 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[41]:

- **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 through effective leadership and engagement, improving culture and capability, strengthening accountability and by being innovative.

Data, Digital and Information[42]:

- **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, including to reputation.
- **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

---

[41] *Orange Book:*
People Risks*; risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviours, the unavailability of capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance.*

[42] *Orange Book:*
Technology Risks*; risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.*
Security Risks*; risks arising from a failure to prevent unauthorised and/or inappropriate access to the estate and information, including cyber security and non-compliance with GDPR requirements.*
Information Risks*; risks arising from a failure to produce robust, suitable and appropriate data/information and to exploit data/information to its full potential.*

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[43]:

- **ICO Policies and Procedures**: Whilst we have an **averse** appetite to non-compliance with ICO policies where they have a 'must' and clear requirement to follow them, we will take a ***cautious*** risk appetite (*are willing to accept some controllable levels of risks*) when an element of judgment of when a policy applies is required by managers.
- **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.
- **Prioritisation :** 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.
- **Workforce:** We have an ***open*** risk appetite (*are willing to accept elevated levels of risks*) to ensuring we have the right people able

[43] *Orange Book:*
Financial Risks*; risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from investment, failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting.*

People Risks*; risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviours, the unavailability of capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance.*

to be in the right roles at the right time to deliver our strategic priorities.

Regulatory[44]:

- **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 ensuring that we carry out our functions and use our powers in an appropriate, proportionate and lawful way.

Other:

- **Other:** Where an activity does not fall neatly within one of the ICO risk appetite categories or crosses over appetite statements then the existing risk appetite definitions should be used as a guide and direction provided by an Executive Director. In principle, the organisation is receptive to taking difficult decisions when benefits outweigh risks.

Back to Top

[44] *Orange Book:*
***Operations Risks**; risks arising from inadequate, poorly designed or ineffective/inefficient internal processes resulting in fraud, error, impaired customer service (quality and/or quantity of service), non-compliance and/or poor value for money.*
***Legal Risks**; risks arising from a defective transaction, a claim being made (including a defence to a claim or a counterclaim) or some other legal event occurring that results in a liability or other loss, or a failure to take appropriate measures to meet legal or regulatory requirements or to protect assets (for example, intellectual property).*

13. 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 ✓ Prioritisation ✓ 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 ✓ Workforce
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 ✓ ICO Policies & Procedures
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 ✓ Security
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.	

Back to Top

15. Risk Capacity

15.1 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.

Annexes

References:

[The Orange Book 2023]
[Orange Book Risk Appetite Guidance Note]

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
4.5	Annual Review of Risk Management Policy	25/3/24	Caroline Robinson
4.6	Annual Review of Risk Management Policy	24/3/25	Caroline Robinson

Back to Top