Audit & Risk Committee – for discussion

Report title: Risk Management – Orange Book Compliance

Meeting date: 24 April 2025

Time required: 10 mins

Presenter: Louise Byers

RAPID Role: Input and Agree – the Decision role is Management Board

Publication decision: The report can be published internally and externally.

Input requested

Audit & Risk Committee (ARC) are requested to:-

> confirm that they agree with the approach and scope of the assessment used to support our proposed disclosure statement of compliance with the five Orange Book principles and suite of guidance documents for inclusion in the governance statement of the Annual Report.

The proposed disclosure statement will be presented at Management Board for final approval of inclusion within the annual governance statement of the Annual Report and Accounts.

Background and summary

In May 2023 the UK Government published an updated version of the Orange Book and introduced the Risk Control Framework (RCF).

As a public sector organisation, the ICO should have systems for identifying and managing risk suited to its business, circumstances and risk appetite. As such, we are required to disclose compliance with or explain our reasons for departure from the five Orange Book principles, clearly and carefully, in our governance statement accompanying our Annual Report and Accounts. The Orange Book is produced by HM Treasury and sets out required risk management practices.

Disclosure should be on the basis of practice and outcome, rather than policy and intention and the Board should choose how they determine what gets disclosed and the strength of its assurance.

The Government Risk Centre of Excellence (CoE) developed a tool providing various levels of assurance questions for use when assessing adherence with the items underpinning the categories and components in the RCF, aligning to the five principles in the Orange Book:-

A. Governance and Leadership;

B. Integration;

C. Collaboration and Best Information;

D. Risk Management Processes; and

E. Continual Improvement.

Given the size and structure of the ICO, the maturity of our risk management framework, the approach and scope agreed last year was as follows:-

> 2023-24 reporting would be based on the 35 high level risk management assurance questions from Part 1 aligning to the five principles of the Orange Book. It was agreed that we complied with each Principle except for one question in the Governance and Leadership Principle.
>
> 2024-25 reporting would build on our compliance assessment by utilising the Suite of Guidance questions in Part 2 covering:-
>
> - Good Practice Guide : Risk Reporting
> - Risk Appetite Guidance Note
> - Risk Management: Skills and Capability Framework
> - Portfolio Risk Management Guidance

In 2024 the CoE added a further 40 questions against the Orange Book Principles into Part 1 of the RCF tool. These additional questions are optional and designed to provide an additional layer of assurance for compliance (annex 2).

It is proposed that we look to utilise the optional 40 questions at a future date and in addition, seek further assurance from GIAA on our risk management framework.

Outcomes and benefits realised

We have undertaken an assessment against the recommended risk control framework questions to consider our compliance with Part 1, the five risk management principles, and Part 2, the suite of guidance documents. The outcome of this assessment is outlined in Annex 1.

The assessment needs to allow the identification and disclosure relating to the substantive outcomes and features of the organisation that were in place for the majority of the year.

Although it is recognised that there is more work to do to continuously improve the ICO's risk management framework, we believe that we currently comply with each Principle with the exception of:-

- Question 5 in the Governance and Leadership Principle
- Question 8 in the Risk Reporting Good Practice Guide
- Questions 4, 5, 6 & 9 in the Portfolio Risk Management Guidance

Part 1 : Orange Book Principles

Governance & Leadership	Out of a total of 9 questions we comply with 8 and need to explain 1 (question 5)
Integration	We comply with all questions
Collaboration & Best Information	We comply with all questions
Risk Management Processes	We comply with all questions
Continual Improvement	We comply with all questions

Part 2 : Orange Book Suite of Guidance Documents

Good Practice Guide: Risk Reporting	Out of a total of 9 questions, we comply with 8 and need to explain 1 (question 8)
Risk Appetite Guidance Note	We comply with all questions
Risk Management: Skills and Capability Framework	We comply with all questions
Portfolio Risk Management Guidance	Out of a total of 9 questions, we comply with 4 and need to explain 4 (questions 4, 5, 6 & 9). One question (Q3) is not applicable to us.

Recommendation:

Based on the outcome of the bank of questions assessment. We recommended that our disclosure within the Annual Report about risk management includes the following statement: -

> *We consider our practices comply with the requirements of the Orange Book's 5 principles (Part A) and Suite of Guidance documents (Part B), with the exception of two areas. The areas requiring improvement are risk reporting and portfolio risk management: -*
>
> - *We plan to make improvements to tailor our risk reporting over the next financial year to both improve the focus and quality of information on risk to further support decision making; and risk reporting for external publication, which may be helpful for ICO customers to understand our risk control environment.*
> - *Whilst programme and project risks are well managed, portfolio management is relatively new to the organisation and is still embedding, as such, further development of the portfolio strategy in the next financial year will offer opportunities to define and improve risk management at the portfolio level.*
>
> *We plan to continue to make these improvements over the next year to demonstrate a sustained period of compliance with the Orange Book requirements.*

Challenges and decisions requested

Decision requested: Does ARC agree with the approach and scope of the assessment used to support our proposed disclosure statement of compliance with the five Orange Book principles and suite of guidance documents for inclusion in the governance statement of the Annual Report?

- *Challenge Question: Do ARC think the 40 new questions included in Part 1 of the RCF at Annex 2 should be utilised to provide additional support to the disclosure statement for 2024/25?*

Decision requested: Do ARC approve the proposed disclosure statement as recommended for inclusion in the Annual Report?

- *Challenge Question: Do ARC have any comments on the statement? Note that the Risk and Governance Team have followed guidance from the Risk Centre of Excellence team on acceptable disclosures.*
- *Challenge Question: Is the disclosure statement, and assessment undertaken to support this, in line with the internal and external auditors opinion statements in the Annual Report?*

Collaboration and interdependencies

In developing this work, we used assurance from our risk maturity assessments which we have included in Annex 1 to cross-check against our understanding. In undertaking this work we collaborated with Directors and involved our risk management champions who collaborated with operational level colleagues from across the business.

Interdependencies have been identified with the PMO Office and Delivery Team in relation to work required to further improve risk management at Portfolio level.

Next steps and future delegations

Should the requested decision be agreed, the next steps for this work are:

- Present to Management Board for final approval as part of the Disclosure Statement in the Annual Governance Statement.
- Continue with workstreams to ensure compliance with all principles and guidance by March 2026.
- Utilise the additional 40 bank of questions for assurance on our compliance of the Orange Book Principles and, in addition, seek further assurance from GIAA on our risk management framework.

Author: Caroline Robinson

Reviewers: Joanne Butler, Louise Byers

Sign off: Jen Green

List of annexes:

Annex 1 – RCF Questions Assessment Outcomes (Part 1 & 2) Comply or Explain

Annex 2 – Orange Book RCF Bank of Questions November 2024 – not included in pack but available at this link (ICO devices only)

Annexe 2: RCF Questions Assessments Outcomes – Comply or Explain

Compliance with Bank of Questions:

Part 1 : Orange Book Principles

Governance & Leadership	Out of a total of 9 questions we comply with 8 and need to explain 1 (question 5)
Integration	We comply with all questions
Collaboration & Best Information	We comply with all questions
Risk Management Processes	We comply with all questions
Continual Improvement	We comply with all questions

Part 2 : Orange Book Suite of Guidance Documents

Good Practice Guide: Risk Reporting	Out of a total of 9 questions, we comply with 8 and need to explain 1 (question 8)
Risk Appetite Guidance Note	We comply with all questions
Risk Management: Skills and Capability Framework	We comply with all questions
Portfolio Risk Management Guidance	Out of a total of 9 questions, we comply with 4 and need to explain 4 (questions 4, 5, 6 & 9). One question (Q3) is not applicable to us.

Risk Maturity Definitions

We have added in our maturity for each of the principle questions where the questions align to our risk maturity assessment:-

- **Risk Naïve** – No formal approach developed for risk management.
- **Risk Aware** – Scattered silo-based approach to risk management.
- **Risk Defined** – Strategies and Policies in place and communicated. Risk appetite defined.
- **Risk Managed** – Enterprise approach to risk management developed and communicated.

- **Risk Enabled** - Risk management and internal controls fully embedded into the operations.

Risk Control Framework Bank of Questions

The table below provides details for each of the areas of the Orange Book that we are assessing against and includes:

- The assurance question
- Whether we comply with the principle or need to explain,
- Our risk maturity levels where the questions align to our risk maturity assessment,
- Additional comments regarding our work in this area.

Part 1 : Orange Book Principles

A : Governance & Leadership

Question 1: How is the desired risk culture defined, communicated, and promoted? How is this periodically assessed?	Comply	Naïve	Whilst there is more work to be undertaken in this space, we currently define, communicate and promote our risk culture via the following:- • Risk Culture is defined in the Risk Management Policy • Risk Maturity Assessments are undertaken on a regular basis • The above are communicated and promoted through:- ○ work with our Risk Champions, ○ via our Risk Management page on Iris, ○ the Risk Appetite Knowledge Pack, and posts on the Viva Engage Risk Management Community and What If community
Question 2: How do human resource policies and performance systems encourage and support desired risk behaviours and discourage inappropriate risk behaviours?	Comply	Managed	• Career Band Progressions framework encourages desired risk behaviours and our PDRs include performance against our

			values which help to support good risk behaviour Additional policies and training for compliance and 'required learning' are in place, all ICO policies encourage desired risk behaviour and there are policies to deal with deliberate inappropriate risk behaviour.
Question 3: How has the nature and extent of the principal risks that the organisation is willing to take in achieving its objectives been determined and used to inform decision making? Is this risk appetite tailored and proportionate to the organisation	Comply	Defined	• Discussions undertaken with SLT/ET to review principle risks and determine risk appetite levels. This informs the Risk Management Policy and Risk Appetite Statement which is set by Management Board • The Policy and Risk Appetite is set by Management Board following discussions to ensure it is proportionate and meets the needs of the organisation. • Decision making tools refer to Risk Appetite
Question 4: How are the board and other governance forums supported to consider the management of risks, and how is this integrated with discussion on other matters?	Comply	Defined	• ET, ARC & MB supported with risk reports, heat maps and deep dive reviews for corporate risks. • People Committee receive reports on the relevant corporate risks • Other governance forums also receive risk information relevant to their work programme • Report templates provide prompts to allow for risks to be raised and discussed
Question 5: How effective are risk information and insights in supporting decision-making, in	Explain	Naive	This has a wider culture element to ensure that risk information is applied correctly as

terms of the focus and quality of information, its source, its format and its frequency?			part of decision making, which will take longer to embed. We have recognised and have begun to improve the focus and quality of information of risk to support decision making but more work is in progress:- • As part of the Employee Experience programme, decision making workstreams Ensuring that ET & MB are provided with more detailed information on corporate risks
Question 6: How are authority, responsibility and accountability for risk management and internal control defined, co-ordinated and documented throughout the organisation?	Comply	Managed	• Authority, responsibilities and accountabilities are outlined within our Risk Management Procedure, • Risk registers identify risk owners and internal controls, • Risk champions established and trained. • Other specialist risk areas also have responsibility and accountability areas defined including:- ○ Budget Holders Lead Information Management Officers
Question 7: How is the designated individual responsible for leading the overall approach to risk management positioned and supported to allow them to exercise their objectivity and influence effective decision-making?	Comply	Managed	• Director of Risk & Governance ○ has direct access to the Information Commissioner and DCEO but reports into the ED of Strategy and Resources ○ attends all ARC and MB meetings and ET meetings when risk is being discussed ○ also has direct access to the ARC Chair ○ has oversight of Effectiveness Reviews of the decision making bodies

			Should any colleague have any concerns about risk and effective decision making then the Director of Risk & Governance has an ‘open door’ position.
Question 8: How are the necessary skills, knowledge and experience of the organisation’s risk practitioners assessed and supported?	Comply	Defined	• Job Descriptions include risk practitioner skills, knowledge and experience • Internal audit undertakes audit on risk, • Performance management ensures that the Risk Team is kept up to date with relevant risk management info, • Risk Team encouraged to complete ongoing training courses in order to stay up to date Also attend training courses, relevant webinars, risk networks, performance management reviews and internal audit outcomes
Question 9: How has the necessary commitment to risk management been demonstrated?	Comply	Defined	Commitment demonstrated through various platforms including:- • Through blogs of senior leaders, • Workshops carried out with members of SLT, • Regular catch ups with risk champions network members, • Risk registers at a number of levels across the organisation, Prepared to provide healthy challenge to ensure the risk management voice is heard

B : Integration

Question 1: How are risks considered when setting and changing strategy and priorities?	Comply	Defined	Risks are considered via:- • Reports sent to the appropriate governance forum • Risk workshops are carried out with senior leaders • Prioritisation tool • Decision templates • EQIAs, DPIAs, legal advice Project & Programme management of strategy and priorities
Question 2: How are risks transparently assessed within the appraisal of options for policies, programmes and projects or other significant commitments?	Comply	Managed	Risks are assessed via:- • Business cases • Project initiation documents • Within decision making papers Risk procedures, including EQIAs, DPIAs, etc.,
Question 3: How are emerging risks identified and considered?	Comply	Managed	Emerging risks can be identified and considered via a number of routes:- • Risk Escalation process • Risk Champions encourage Directors to include risk as a standing agenda item on management meetings • MB & ET cascade down emerging risks which are then formulated with risk owner • Staff are encouraged to think about risk in their day to day roles and measured through PDR and performance Management framework
Question 4: How are risks to the public assessed and reflected within policy development and implementation?	Comply	Aware	Risks to the public are assessed via:- • Regulatory position and policy development takes account of the main HARMS to public

			Prioritisation of our regulatory activity also takes account of harm
Question 5: How are National Risk Register risks, that are particularly pertinent to the organisation, recognised in risk assessments and discussions?	Comply	Defined	• Risk Team carry out monthly analysis meetings of the National Risk Register and elements of these risks are discussed with relevant risk owners of corporate risks Reports sent to SLT for information and assurance on work carried out

C : Collaboration and Best Information

Question 1: How is an aggregated view of the risk profile informed across the organisation, arm’s length bodies and the extended enterprise supporting the delivery of services?	Comply	Naive	• Risk profile for corporate risks regularly reported to SLT, ET, ARC and MB and published internally as part of the paper publication process • Corporate Risk and Opportunity Register and Heat Maps linked to the Risk Management page on the intranet • Risk Champions are also able to view and feedback locally on the corporate risks Local level directorate risk registers are reviewed and the top 3 risks are reported to ET.
Question 2: How are the views of external stakeholders gathered and included within risk considerations?	Comply	Naive	• Gathered by risk owners by their interactions • Take account of research material gathered from stakeholders that would need to feed into any corporate risks • Risk indicators identified for each corporate risks • Threat assessments received are taken into consideration for cyber security corporate risk

			• Where appropriate consultations are undertaken • Feedback mechanisms, eg., complaints and suggestions Have a media monitoring service to identify possible reputational risks at an early stage
Question 3: How does communication and consultation assist stakeholders to understand the risks faced and the organisation's response?	Comply	Naive	• Our commitment to transparency means we are open not only about decisions we take, but also why we take them. • John's speeches often focus on how we prioritise work and explain the approaches we are taking. We amplify these through social media promotion. • Our website has a wealth of information that explains our approach and structures, from the publication of meeting minutes through to our FOI disclosure log • Gathered by risk owners through their interactions with Stakeholders Regular meetings take place with our sponsoring department to discuss risks and responses
Question 4: How is function and professional expertise used to inform strategies, plans, programmes, projects and policies?	Comply	Defined	• All staff are encouraged to abide by ICO values including collaboration so for any of these areas they should ensure that they collaborate with functions and experts to draw on expertise to inform work/decisions • Healthy challenge through governance process to ensure that they have collaborated adequately • Decision making report template

			• Roles and responsibilities for experts in programmes/projects Business Case / PID process
Question 5: How do expert functions and professions inform the identification, assessment and management of risks and the design and implementation of controls?	Comply	Managed	• Regular risk review meetings carried out with risk owners of the corporate risks to ensure regular review and correct mitigations Advice sought from experts to assist in the risk update
Question 6: How are functional standards communicated and their adherence monitored across the organisation?	Comply	Defined	• Communicated to relevant directors, initial review to ensure meeting 'good' criteria for all functional standards Outcomes reported to ARC

D : Risk Management Processes

Question 1: How are risk taxonomies or categories used to facilitate the identification of risks within the overall risk profile?	Comply (with more work to do)	n/a	• Risk Management Procedure recommends that from an external perspective that we use the PESTLE tool • Currently categories are under corporate objectives and categories for risk appetite It is recognised that there is more work to do to embed the use of categories
Question 2: How are risk criteria set to support consistent interpretation and application in assessing the level of risk? How effective are these in supporting the understanding and consideration of the likelihood and consequences of risks?	Comply	n/a	• Risk criteria are set as part of Risk Management Procedure and reviewed on an annual basis. • The criteria is outlined within the scoring chart and feedback of usefulness of the criteria is gained via 121 update meetings with risk owners Criteria is effective because the risk articulation includes cause, threat and impact as part of risk description

Question 3: How are limitations and influences associated with the information and evidence used with risk assessments highlighted?	Comply	n/a	• Worst case assumptions used and comments recorded to help with the assessments Moderation is undertaken at ET/ARC and challenge provided on assumptions
Question 4: How are interdependencies between risks or possible combinations of events (‘domino’ risks) identified and assessed?	Comply	n/a	• Interdependencies with corporate risks are identified with risk owners during risk review meetings Any significant relationships between risks are highlighted in update reports
Question 5: How dynamic is the assessment of risks and the consideration of mitigating actions to reflect new or changing risks or operational efficiencies?	Comply	Managed	Fairly dynamic:- • Review of mitigating actions and future planned actions carried out at every risk review meeting Risk owners encouraged to let Risk Team know if anything changes with the risk between review meetings
Question 6: How are exposures to each principal risk assessed against the nature and extent of risks that the organisation is willing to take in achieving its objectives – its risk appetite – to inform options for the selection and development of internal controls?	Comply	Defined	• Risk Appetite discussed and agreed with risk owner and moderated by Executive Director. • Risk appetite and tolerance checked at gross risk rating, current risk rating, expected risks rating and target score at every corporate risk review meeting Risk Champions trained on applying risk appetite for Directorate Risk Registers
Question 7: How are decisions made in balancing the potential benefits of the design and implementation of new or additional controls with the costs, efforts and any disadvantages of different control options?	Comply (corporate risks)	Managed	• If cost of mitigating risk is quite significant then Directorate level risks would be expected to be escalated and discussed with Executive Director. • At corporate risk level this would be discussed with ET.

			• In the main, the decisions are made in line with RA for the risk area
Question 8: How are contingency arrangements for high impact risks designed and tested to support continuity, incident and crisis management and resilience?	Comply	Naive	• Forms part of the Business Continuity programme and exercises are designed to test the high impact and most likely scenario given current conditions eg., in winter, testing winter related risks, etc • A number of these will also be tested at a local level with the assistance of the Business Continuity Champions
Question 9: How is the nature, source, format and frequency of the information required to support monitoring of risk management and internal control defined and communicated?	Comply	n/a	Defined within the Risk Management procedure which is communicated via:- • Held on our intranet site in the Policies Hub, • Communicated via the Governance & Planning Hub • Communicated with Risk Champions • Communicated at various senior leadership briefings • Utilising specific internal comms on Iris and Weekly Word, eg., fraud risk
Question 10: How are new and changing principal risks highlighted and escalated clearly, easily and more rapidly when required?	Comply	Defined	• Escalation Procedure in place and linked to the Risk Management page • Risk Team is contactable via dedicated inbox. • Risk Team will discuss emerging risks with risk owners and provide support in drafting and scoring the risk Risk Team would be able to escalate risks to ET immediately if required
Question 11: How comprehensive, informative and coordinated are assurance	Comply	Managed	• The internal audit programme is based on corporate risks,

activities in helping achieve objectives and in supporting the effective management of risks?			- Self-assessment through government functional standards. - Compliance assessment work carried out. - External audit who liaise with internal audit on coordinating assurance activity - Assurance map and interdependencies identified across corporate risks - Various assurance reports sent to People Committee, ARC and MB Liaison with Risk Champions
Question 12: How do disclosures on risk management and internal control contribute to the annual report being fair, balanced and understandable?	Comply	n/a	The annual report gives an overview of our key risks and how they have been managed over the last year, along with the assessment of the overall control framework from our internal auditors. This gives an even-handed view of how risks have been approached, managed, and changed over the year, as well as areas where additional assurance has been gained through internal audits.

E : Continual Improvement

Question 1: How are policies, programmes and projects evaluated to inform learning from experience? How are lessons systematically learned from past events?	Comply	Aware	- Do own lessons learned and at each review of policy & programmes. Colleagues are encouraged to share learned experiences through the career progression and value statements
Question 2: How is risk management maturity periodically assessed to identify areas for improvement? Is the view	Comply	Aware	- A risk maturity assessment recently carried out via a questionnaire to Senior and Middle managers and followed up with

consistent across differing parts or levels of the organisation?			interview style questions and responses captured. Recognised that more consistency with risk management is required and an action plan for this is in place
Question 3: How are improvement opportunities identified, prioritised, implemented and monitored?	Comply	Aware	• General feedback during the year, through risk champions, also feedback from ARC and MB. • Prioritised in terms of immediate change or wait until procedure is due to be updated. • Monitored alongside the rest of the framework. Goals within the policy - reported on regularly to ARC

Part 2 : Orange Book Associate Suite of Guidance Documents

Good Practice Guide : Risk Reporting

Question 1: Is the risk reporting aligned and informed across the organisation, its partners and its stakeholders?	Comply	n/a	• Organisation; risk reporting aligned internally at Delivery Group, Executive Team, Audit & Risk Committee and Management Board • Stakeholders; reporting in the Annual Report • Partners; Corporate Risk Register shared regularly with DSIT
Question 2: Is the risk reporting evidence based, making good use of the management information and expertise available?	Comply	n/a	• Evidence based in terms of action and activities to mitigate the risks • Additional work planned for management information including risk indicators

Question 3: Does it contain the information required by the reader to make decisions or participate in productive discussions?	Comply	n/a	•Report templates guide report writers to consider risks in their decisions, discussions •Productive discussions encouraged through our “matters to consider” in risk update reports
Question 4: Does the risk reporting support informed decision-making and prioritisation activity?	Comply	n/a	As above
Question 5: Does the risk reporting promote: • A clear understanding of risks? • Provide a confidence assessment in the treatment of risks? • Prompt corrective actions? • Support informed decision making?	Comply	n/a	•This is currently undertaken at a Corporate Level. There is more work to develop at an operational level
Question 6: Is the risk reporting integrated with other governance discussions and processes, including but not limited to planning and performance management and the insights provided across the “lines of defence”?	Comply	n/a	•Integrated with compliance report •Directorate risk registers integrated with business plans •Assurance mapping includes Government standards •Integrated with our work on business continuity, fraud risk assessments and Information Risk & Governance Group
Question 7: Does the risk reporting provide a suitable context to support the robust assessment of an organisation’s principal risks, by providing an accurate: • Internal perspective, • System-wide perspective • Update on current macro-environmental concerns, and • Horizon scanning information?	Comply	n/a	•Internal; Corporate and Cross Cutting Risk Registers in place •Risk Management Procedures encourages risk managers to think about wider perspectives including impact on other areas of the business •Macro environmental concerns considered and reported on where necessary as part of corporate risk assessments

Question 8: Is the risk reporting tailored to provide the information required by customers?	Explain	n/a	•More work could be undertaken to tailor our risk reporting for external publication which may be helpful for ICO customers to understand our risk control environment •Plans in place to expand risk reporting in the Annual Report
Question 9: Does the reporting provide a clear summary and confidence assessment of the risks to the organisation?	Comply	n/a	•This is provided through our regular risk update reports, heat maps and through deep dives into corporate risks

Risk Appetite Guidance Note

Question 1: Have departmental boards determined and are continuously assessing the nature and extent of the principal risks that the organisation is exposed to and is willing to take to achieve its objectives – its risk appetite – and ensure that planning and decision-making reflects this assessment?	Comply	Defined	Reviewed on an annual basis by Executive Team and Management Board
Question 2: Has the organisation clearly set out both the target and acceptable position in the pursuit of its strategic objectives?	Comply	Defined	The Corporate Risks are reviewed continuously with risk owners
Question 3: Has the organisation clearly set out both the target and acceptable position in the pursuit of its strategic objectives?	Comply	Defined	The Corporate Risks are reviewed continuously with risk owners
Does the organisation have an overarching risk appetite statement?	Comply	n/a	We have multiple risk appetites for different business areas within the Risk Appetite Statement
Question 4: Have organisation developed statements which describe their attitude, at a point in time, to accepting risk in each of their areas of principal risk?	Comply	Defined	Combination of risk appetites and principle risks on the corporate risk register being discussed with risk owners

Risk Management : Skills and Capability Framework

Question 1: Does the organisation have a designated individual responsible for leading the organisation's overall approach to risk management?	Comply	Managed	•Director of Risk & Governance •Head of Risk & Governance Risk & Business Continuity Manager
Question 2: Are risk management professionals in place responsible for managing and implementing the risk management framework effectively and consistently across the organisation?	Comply	Managed	•Head of Risk & Governance Risk & Business Continuity Manager
Question 3: Is risk management being used by the organisation to make informed decisions, and enable the pursuit and achievement of objectives and outcomes?	Comply	Defined	Whilst we comply there is more work to be undertaken, as highlighted by our Risk Maturity Assessment
Question 4: Are the appropriate skills in place to ensure that the organisation is building its risk management capability and culture?	Comply	Defined	Currently at Senior Leadership Level however more work can be undertaken at operational levels, including our risk management training modules
Question 5: Are the risk management professionals core tasks and technical competencies used to assist in the continual development and training of risk professionals?	Compy	Defined	Head of Risk & Governance and Risk & Business Continuity Manager have completed the required training to gain the Government Risk Accreditation

Portfolio Risk Management Guidance

Question 1: Are the different risk aspects in portfolios as defined in the Portfolio Risk Management guidance adequately considered throughout the lifecycle of the portfolio?	Comply	n/a	•Portfolio formation - risk analysis included in programme case. •Portfolio governance - Delivery Group, mothly dashboard incl risk register + milestone report

			•Effectiveness tracking - additional MI to assess risk reduction eg DP fee income •Risk profilling - programme level risk and control assessments collated for consideration in aggregate, at portfolio level as part of the portfolio risk register and management performance dashboards. •Materiality and risk appetite - though the portfolio is cognisant of the ICO's risk appetite, we haven't yet set the levels of materiality and associated risk appetite which are appropriate for the overall portfolio. •To/in/of risk profiling - this is not yet mature and will form part of the portfolio risk management Risk management roles - in place. Additional SRO training planned.
Question 2: Are risk implications appropriately considered during the creation of portfolios and when appraising investments?	Comply	n/a	Portfolio formation – risks analysis included in programme case
Question 3: Are mechanisms for making cross-boundary decisions, including decisions on prioritisation clarified in advance for cross boundary portfolios?	N/A	n/a	We don’t have cross-boundary portfolios
Question 4: Is the effectiveness of interventions in managing risk regularly tracked and the information used to shape and drive portfolio actions and decisions?	Explain	n/a	Projects and programmes manage risk via risk registers, however effectiveness of interventions are not routinely or consistently tracked.
Question 5: Does the portfolio profile chances of degrees of variation in intended outcomes	Explain	n/a	The portfolio doesn't yet profile chances of degrees of variation in intended outcomes

relating to cost, time, benefits and other objectives using appropriate qualitative and quantitative techniques?			relating to cost, time, benefits and other objectives using appropriate qualitative and quantitative techniques
Question 6: Is the risk appetite of the portfolio clearly understood and in line with the wider risk appetite of the parent organisation?	Explain	n/a	Risk appetite is currently set at programme level, and aligned with the organisational risk appetite (for example within two different programmes we may have a hungry risk appetite to innovative technology, but a cautious risk appetite to compliance) Further development of the portfolio strategy in FY 25/26 offers opportunities to define the portfolio, and set risk appetite against core portfolio outcomes.
Question 7: Are external risks and dependencies to the programme/project and risks and dependencies of the programme/ project to others well understood and effectively managed?	Comply	n/a	In line with the ICO's Risk and Opportunity Management procedure, all Programme and Project Boards should identify risks which could have an impact on achieving portfolio, programme, project objectives. All programmes, projects have clearly defined objectives, and a risk register and use techniques such as PESTLE analysis to identify potential external risk. Dependencies are managed via weekly portfolio oversight meetings which review risks and dependencies across the transformation programmes.
Question 8: Are risk management roles and responsibilities clearly defined across the portfolio?	Comply	n/a	Risk management roles defined in ICO Risk and Opportunity Management procedure (p.7) SRO training planned for Q1 25/26
Question 9: Are risk related data challenges understood and adequately considered when	Explain	n/a	Risk related data challenges are not formally considered when designing the governance

designing the governance and reporting arrangements for the portfolio?			and reporting arrangements for the portfolio.