Government
Finance
Function

Risk Appetite Guidance Note

August 2021
V2.0

Contents

1. Introduction

1.1. The Orange Book – Management of Risk, Principles and Concepts (2020) advises 'the Board should determine and continuously assess 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. Effective risk management should support informed decision-making in line with this risk appetite, ensure confidence in the response to risks, transparency over the principal risks faced and how these are managed'. This guidance has been developed by risk practitioners in the public sector to support colleagues in implementing effective risk management arrangements, aligned with the Orange Book principles.

1.2. Public sector organisations cannot be culturally risk averse and be successful. Effective and meaningful risk management in government remains more important than ever in taking a balanced of risk and opportunity in delivering public services. Risk management is an integral part of good governance and corporate management mechanisms. An organisation's risk management framework harnesses the activities that identify and manage uncertainty, allows it to take opportunities and to take managed risks not simply to avoid them, and systematically anticipates and prepares successful responses. A key consideration in balancing risks and opportunities, supporting informed decision-making and preparing tailored responses is the conscious and dynamic determination of the organisation's risk appetite.

1.3. This guidance has been developed to provide key considerations for organisations to apply when formalising and strengthening their existing practices to support and inform decision-making.

1.4. Whilst there is wide-ranging guidance on the development of risk appetite statements, much of it is focused on the financial services sector. Clear and helpful risk appetite statements are more easily developed in organisations which can apply consistent units of measure to inputs and outcomes and can look at aggregated portfolio risks in these units, such as £x. Just as there are different approaches taken to the development of risk appetite statements in the private sector, development in the public sector requires a considered approach to reflect that public services realise value to diverse timeframes and utilise varied units of measure to assess public value in their outcomes.

1.5. The concept of risk appetite is further challenged in public sector organisations by the need to demonstrate, often over a spending period, that public funds achieve value for money. Risk appetite helps organisations establish a threshold of impacts they are willing and able to absorb in pursuit of objectives, which may include but is not limited to financial loss. This concept of calculated risk and acceptable loss may be difficult to reconcile with the nature of many public services. If properly applied and maintained, however, understanding risk appetite results in improved organisational health, as trade-offs are made allowing resources to be prioritised and allocated where most needed to support the management of risks to achieving objectives, whilst maintaining performance and demonstrating value for money (see 6.5 and 6.6 below).

1.6. The good practice guidance outlined in this document can be used to direct decision-making at the point investment and prioritisation choices are made, as well as in management's periodic reviews of risks and performance. The good practices detailed in this guide have been gathered from experience across the Civil Service risk management community. They have been tested through practical application and have been proven especially beneficial in times of heightened uncertainty and rapid change, such as the Covid-19 pandemic, when decisions need to be made quickly and often with incomplete information.

1.7. This guide should be considered alongside the Orange Book and other associated good practice guides. These documents can be accessed via Gov.uk or OneFinance.

1.8. The Government Finance Function is grateful to all involved in the production of this guide. A full list of contributors is provided at Annex B. Particular thanks is given to Simon King from the Ministry of Defence, who chaired the working group that developed this guidance.

2. Assumptions

2.1. This guide has been developed to support organisations to implement the concepts and principles outlined in the Orange Book. The information provided in this guidance is framed around the assumption that an organisation's risk framework aligns with the Orange Book.

2.2. To maximise the benefit of this guidance, organisations should recognise the following:

- While desirable, it is often not possible to manage all risks at any point in time to the most desirable level, but the discipline and approach set out in this guidance provide a means to manage risks to a tolerable level
- Outcomes cannot be guaranteed when decisions are made in conditions of uncertainty
- It is often not possible, and not financially affordable, to fully remove uncertainty from a decision or in the design and application of control activities
- Decisions should be made using the best available information and expertise
- When decisions need to be made urgently, the information relied upon and the considerations applied to it should, as in the normal course of business, be retained
- The risk culture must embrace openness, support transparency, welcome constructive challenge and promote collaboration, consultation, co-operation and continual improvement

2.3. The best available evidence should be used to inform all decisions and this guidance recognises that organisations may have areas of risk which are data-rich, can apply automated scientific judgement or are dependent on the subjective judgement of the best available experts. Each organisation should adopt the most appropriate approach for its needs.

3. What is risk appetite?

3.1. Risk appetite as a concept is often referenced in organisations, without clearly defining what it is. Similarly, the terms risk appetite and risk tolerance are often used interchangeably. It is equally true that many organisations already apply the principles contained in this guidance without necessarily fully acknowledging them as part of a risk management framework where risk appetite is actively considered in decision-making.

3.2. When referenced in this guide, risk appetite will be referred to as a concept. Within this concept, we will refer to optimal risk and tolerable risk positions using the following definitions:

- **Optimal risk position:** the level of risk with which an organisation **aims** to operate.
- **Tolerable risk position:** the level of risk with which an organisation is **willing** to operate.

The diagram below demonstrates the interaction between these concepts.

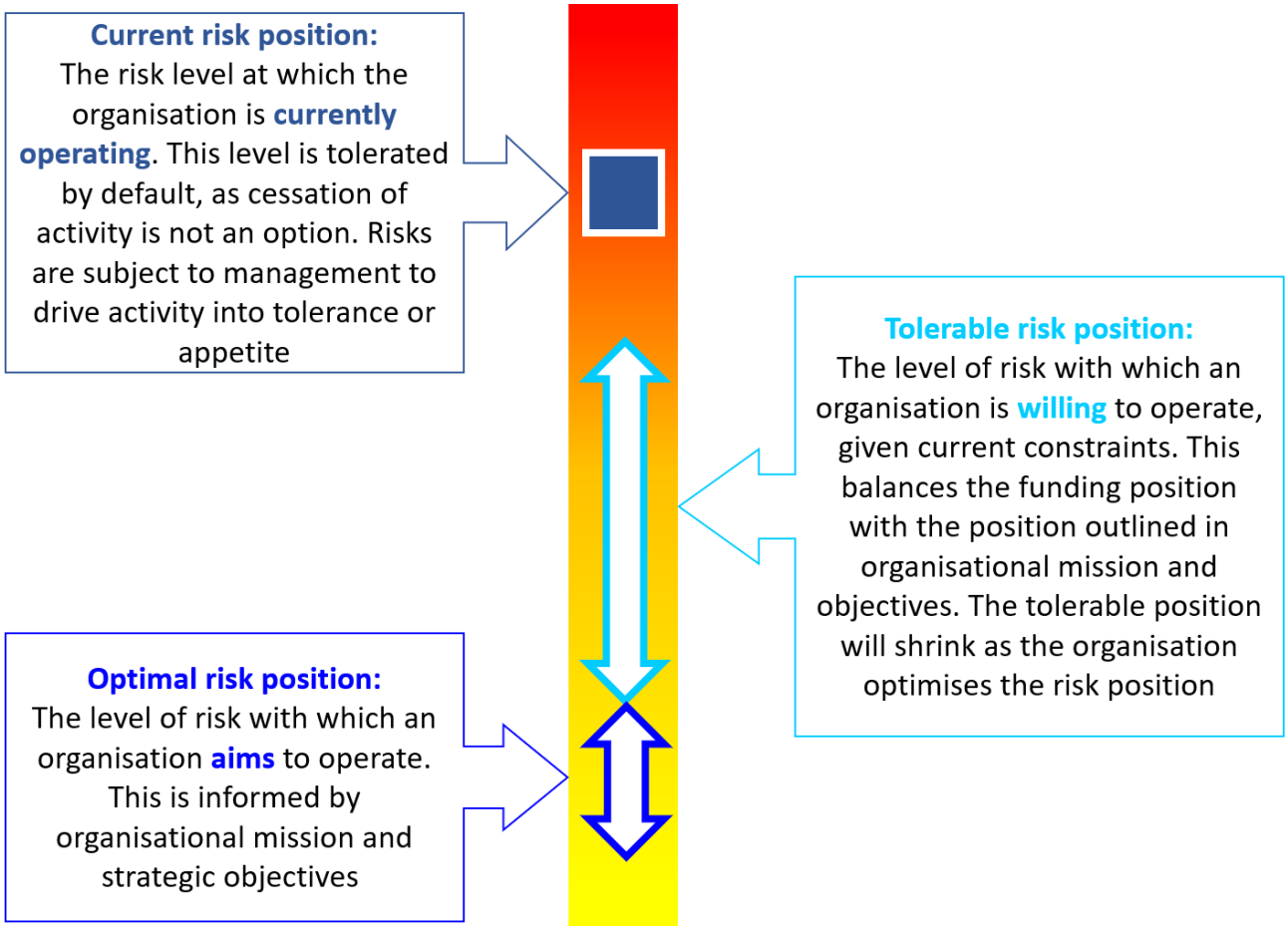

Figure 1.

Please note: The definition of tolerable risk in this guide relates specifically to an organisational position. A tolerable risk position should not be confused with tolerating a risk, by choice, as a risk response: An organisation may be tolerating a risk which sits within the tolerable or optimal positions. Each organisation will have its own scale of risk acceptance and this guide is not suggesting that a risk appetite or tolerance position must be set to a low / green position on local risk assessment scales.

4. Why is risk appetite important?

4.1. Risk appetite provides a framework which enables an organisation to make informed management decisions. By defining both optimal and tolerable positions, an organisation clearly sets out both the target and acceptable position in the pursuit of its strategic objectives. The benefits of adopting a risk appetite include:

- Supporting informed decision-making
- Reducing uncertainty
- Improving consistency across governance mechanisms and decision-making;
- Supporting performance improvement
- Focusing on priority areas within an organisation
- Informing spending review and resource prioritisation processes.

5. Risk appetite development

5.1. When developing its risk appetite, an organisation needs to consider the norms of the environment and the sectors in which it operates, its own culture, as well as governance and decision-making processes.

5.2. The application of a more technical and quantitative approach, utilising specialised terms, can be beneficial in some circumstances and within risk mature organisations. In organisations where the risk management culture is being developed and embedded, this approach may be counterproductive. In these instances, the application of simplified terminology may improve engagement, as colleagues may be more willing to participate in a process positioned as informed decision-making, rather than more formalised organisational risk management. People may be less inclined to engage with overly technical language about taking risks, but instead may be more comfortable and confident talking about making informed and balanced decisions. This may be more important in instances where there is clear uncertainty and/ or where the information available to inform the decisions is recognised as imperfect but the best available.

5.3. Those responsible for risk management should assess organisational maturity and develop an appropriate response which will deliver the benefits of a risk appetite approach to communicate expectations, inform decisions and enhance outcomes. This may be badged as a decision framework rather than a risk appetite statement, although the latter will continue to be referenced in this document.

5.4. The following principles should be considered and applied when developing an organisational approach to risk appetite:

- In addition to having an overarching risk appetite statement, organisations should develop statements which describe their attitude, at a point in time, to accepting risk in each of their areas of principal risk[1]. These should include an optimal and tolerable position and should provide coverage and link to each of the organisation's principal risks. An example is provided in Section I of Annex A. A list of the Orange Book recommended risk categories is provided in Section II of Annex A

[1] The Orange Book – Management of Risk, Principles and Concepts Annex 4 – Example Risk Categories. See also Section II of Annex A..

- Organisations should determine their areas of principal risk in relation to their purpose, resources and the views of their stakeholders. It is recommended these areas are considered using the risk categories detailed in the Orange Book
- Risk appetite statements should:
    - provide a structure for an organisation to work within. When correctly applied, statements describe acceptable outcomes relating to decisions being taken. An example is provided in Section III of Annex A
    - drive thinking about results and outcomes the organisation seeks to realise, as well as about what would need to change if outcomes were not acceptable
    - describe the organisation's typical challenges and the basis on which different outcomes are justified
    - describe the organisation's acceptable behaviour in reasonable circumstances. In circumstances where a decision is to be made and there are no directly comparable situations, risk appetite statements can provide illustrative guidance that can be adapted, documented and applied
    - be set against a sliding scale, with descriptors which are relevant to the organisation. Illustrative examples are provided in Section IV of Annex A. This scale should demonstrate and reinforce the range of outcomes that are acceptable in different situations, and should be separate[2] from scales used to assess the likelihood and impact of a risk
    - be dynamic and updated as necessary to reflect any significant changes in the context their organisations operate within, whether driven by societal, economic or political changes, for example
- While a single statement can be used to describe an organisation's current appetite for risk in a particular risk category, it may be useful to describe relevant specific areas within this. When speaking about financial risk, for example, it would help to explain the different approaches the organisation takes to fraud and propriety. See Section III of Annex A for examples
- Facilitated sessions engaging stakeholders, including Function leads as appropriate, are required to support the development of optimal and tolerance levels. This approach may range from in-depth processes involving wide ranging stakeholder engagement, to focused engagement with senior management. This guidance recommends direct senior engagement, focused on developing agreed descriptions of acceptable behaviours and outcomes, as an efficient approach which ensures buy-in at the senior level. Ultimately, the Board should determine and continuously assess its risk appetite and agree the descriptions
- Most organisations will already set a 'target' risk assessment which they aim to reach through combinations of improvements in existing controls and the introduction of new ones. If this target level of risk is aspirational and not connected to known activities that are already funded and in progress, or to plans with clear outcomes, actions and agreed funding, this may already represent the organisation's optimal position. However, if the target risk assessment only reflects what is currently achievable, the organisation's optimal position for a particular risk may be identified as lower or may be revealed to be higher in which case some of

[2] Risk assessment scales typically describe illustrative outcomes whereas a framework for informing decisions requires a greater future-focus and recognition of context around the decision.

the planned improvements can be stopped and the resources put to more effective use elsewhere

- Organisations should specify whether their appetite statements apply to a risk's inherent or residual assessment, the examples in the annex deliberately include both. If a particular risk appetite is expressed as wanting to avoid inherent risk, it is likely that decisions which have any uncertainty will need to be avoided. However, if the risk appetite is expressed in terms of residual risk, then decisions with uncertain outcomes can be taken, but will require assurances that the level of associated risk can be limited to that described
- In addition to the periodic review of individual and aggregated risk assessments, indicators can be developed to alert management to probable changes in a risk which
  - confirm that actions agreed to move a risk in a particular direction are having their intended effect
  - could prevent it from exceeding previously agreed tolerance levels; or prevent it from being managed to unnecessary levels beyond the optimal position

5.5. As organisations consider and maintain their risk appetite to reflect context and changing environmental factors, there may be circumstances, such as those experienced dealing with government's response to the Covid-19 crisis, when it becomes necessary to significantly alter the level, nature and balance of risks with which an organisation is willing to, or is required to, operate to deliver public services for a period of time. Where this occurs, it is important that there is openness and transparency of these decisions and arrangements, active monitoring and reporting of consequences and clarity over recovery actions. If necessary easement decisions are one-off exceptions, they should be documented and available for scrutiny. If the circumstances are expected to endure, if only temporarily, then the organisation should consider re-stating its optimal and tolerable positions for risk in these areas and reviewing this regularly.

6. How should risk appetite be applied?

6.1. The Orange Book describes risk management as an essential part of governance and leadership, and fundamental to how an organisation is directed, managed and controlled at all levels. The application of an organisational risk appetite, subject to consideration at appropriate decision making and governance bodies, is necessary for this. Section A of the Orange Book describes the role of risk management within governance and leadership arrangements as follows: 'Risk should be considered regularly as part of the normal flow of management information about the organisation's activities and in significant decisions on strategy, major new projects and other prioritisation and resource allocation commitments'[3]. As part of decision-making, an organisation's considerations should include whether:

- Intended benefits justify the range of outcomes
- The plausible outcomes are within the current appetite
- Available resources can be reallocated, if necessary, to allow benefits to be realised within the stated appetite

[3] The Orange Book – Management of Risk, Principles and Concepts Section A - Paragraph A5

- The consequences of taking a decision which could be outside the organisation's optimal or tolerable risk positions have been transparently accepted within the organisation's delegation framework

6.2. As part of the organisation's planning processes, therefore, it should consider the degree of certainty with which available resources can realise strategic or policy outcomes and whether any gap is within its risk appetite. Similarly, if resources are being reallocated as investment is re-balanced, any change in performance levels or confidence over outcome delivery should be reviewed against its risk appetite.

6.3. Risk appetite statements outlining optimal and tolerable positions are key enablers to communicating expectations and ensuring effective decision-making. They should be considered robustly and consistently across an organisation. In addition, their consideration may form evidence to inform and support Spending Review processes, as well as internal prioritisation, investment and budget allocation processes.

6.4. To identify the category of risk appetite guidance which would be most appropriate to inform a decision being made, the following should be considered:

- The Orange Book example risk categories in Section II of Annex A suggest a useful taxonomy for organising risks and provide illustrative descriptions of underlying causes
- The example risk statements, by category in Annex A, again use the Orange Book categories but instead describe the levels of consequence or approach to control that an organisation might want to adopt

6.5. The consequences of a decision being considered might be assessed as impacting several areas, perhaps even in a particular order, and require consideration of risk trade-offs between differing aspects. In this case the organisation would need to document what was considered, at the time, to inform the decision and the balance within the judgement made. For example, an organisation with a perceived high risk of service delivery failure might have an investment choice to make which would significantly reduce capacity in the resource budget. If this organisation has a very low (opposed/averse) appetite for risk in relation to annual resource limits and value for money, and a low (minimalist) overall appetite for risk to service delivery, its decision should, among other things, consider:

- The level of improvement in service delivery that is sought from the resources required and the effect of this on the level of risk exposure
- Whether the realisation of benefits can be assured to support the value for money decision
- Whether any increased costs that would be associated with remediating service delivery risk, represent appropriate value for money
- The balance between managing resource risk and managing service delivery risk
- Whether additional monitoring is able to be used to help manage any risk of increased financial pressure, if the investment is made, or the remaining risk to service delivery if the investment is not made

6.6. It is not always practical or affordable to fully manage risks to the level of an organisation's optimal position and the application of the principles in this guidance provide a pathway for doing so. When decisions are made outside of appetite (which increase risk beyond the optimal or tolerable positions), their justification and evidence should be recorded including, if appropriate, seeking Ministerial Direction. If a decision recognised as being outside of appetite is considered necessary, and is appropriately authorised and approved, it might be appropriate to require specific monitoring and assurance conditions to be set.

7. Review of risk outcomes

7.1. Within the public sector, the nature of the services provided, changing external demands and fiscal constraints mean it is neither feasible nor practical to fully prevent or mitigate all risks at any point in time.

7.2. Individual organisations may find, if they have meaningful assessments of the uncertainty they face, that they are required to carry more risk than is desired. In this case, as per Figure 1, an organisation must assess if the risk is within organisational tolerance levels, or whether active interventions are required to guide the organisation closer over time towards the optimal position, outlined in the appetite statements.

7.3. Risk appetite statements help to inform resource allocation at decision points, and additionally when the organisation periodically reviews its performance. The following principles should be applied in conducting this review:

- Organisations should consider what level of outcomes the best available performance information suggests they will achieve and how this informs their assessment of uncertainty and risk
- Organisations should periodically consider whether the latest assessment of its risks, both individually and aggregated into their exposure areas, is in line with its appetite for risk in those areas
- Risk appetite statements should not be re-baselined to change the perception of tolerated risks, but organisations should consider whether the assumptions behind their previous statements remain valid and whether the organisation might, of necessity, need to recognise an increased optimal risk position
- Organisations should consider how available resources can most effectively be reallocated to improve assessments of either individual risks or a category of risk, or a combination of both
- In choosing which risks or categories of risk to prioritise bringing back into or towards its optimal position, organisations will need to consider the difference that available resources can make on the impact, likelihood or the speed with which the effects of a risk event would be experienced, and which would most improve the deliverability of outcomes
- If no actions are being taken to improve the profile of a risk which is being tolerated outside of appetite, or there is no urgency for improvements to be realised, the organisation should consider[4] whether this suggests its real appetite for the risk and

[4] Other risk management processes detailed within the Orange Book will have provided assurance that the assessments of risk are accurate.

whether decisions to allocate resources to lesser risks should be reviewed. These considerations should be documented

- It is neither feasible nor practical to fully prevent or mitigate all risks and some, which are beyond the stated appetite, might at times need to be tolerated and actively monitored

8. Auditing risk appetite

8.1. As a key part of the risk management framework, and to inform an opinion on the adequacy and effectiveness of governance, risk management and internal control , it is likely that an organisation's internal auditors will want to review how its risk appetite statements were developed and how they are applied in practice within decision making and the design and operation of control activities.

8.2. It is recommended that organisations document the factors influencing the decisions they make to ensure transparency and be able to demonstrate the exercise of judgement in seeking to deliver value for money.

8.3. Internal auditors may want to review evidence of:

- The organisation's Board considering and agreeing to the risk appetite statements;
- The way the organisation sets out to make decisions: how it assures itself that it follows its own policy, records the context and information that was available at the time, and how the risk appetite statements and other factors were considered, including risk trade-offs;
- The nature and level of risk which management acknowledged was being accepted and how they set escalation parameters and monitoring arrangements to be assured that any conditions set were met; and
- The organisation periodically reviewing its risk appetite statements and that, when doing so, it documents that it had considered whether it had all the information necessary to support and enable this effectively.

9. Further information

9.1. For more information, or to provide feedback on this guidance, please email GovFinance@hmtreasury.gov.uk.

9.2. Information on the development of Orange Book Good Practice Guides can be found on OneFinance. Please refer to the Heads of Risk Network pages for the latest news.

Annex A: Risk appetite tools

The following tools have been developed by the Civil Service risk community to support the implementation of an organisational risk appetite.

I. **Example levels defined by risk appetite categories**

II. **Orange Book example risk categories**

III. **Example risk appetite description**

IV. **Risk appetite scales**

I. Example appetite levels defined by risk categories.

The following table provides a sample of risk appetites developed against a selection of the risk categories recommended in Annex 4 of the Orange Book. A full list of the Orange Book recommended categories is provided in Section II of Annex A.

Risk appetite level definition					
	Averse	**Minimal**	**Cautious**	**Open**	**Eager**
Strategy	Guiding principles or rules in place that limit risk in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 5+ year intervals	Guiding principles or rules in place that minimise risk in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 4-5 year intervals	Guiding principles or rules in place that allow considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 3-4 year intervals	Guiding principles or rules in place that are receptive to considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 2-3 year intervals	Guiding principles or rules in place that welcome considered risk taking in organisational actions and the pursuit of priorities. Organisational strategy is refreshed at 1-2 year intervals
Governance	Avoid actions with associated risk. No decisions are taken outside of processes and oversight / monitoring arrangements. Organisational controls minimise risk of fraud, with significant levels of resource focused on detection and prevention.	Willing to consider low risk actions which support delivery of priorities and objectives. Processes, and oversight / monitoring arrangements enable limited risk taking. Organisational controls maximise fraud prevention, detection and deterrence through robust controls and sanctions.	Willing to consider actions where benefits outweigh risks. Processes, and oversight / monitoring arrangements enable cautious risk taking. Controls enable fraud prevention, detection and deterrence by maintaining appropriate controls and sanctions.	Receptive to taking difficult decisions when benefits outweigh risks. Processes, and oversight / monitoring arrangements enable considered risk taking. Levels of fraud controls are varied to reflect scale of risks with costs.	Ready to take difficult decisions when benefits outweigh risks. Processes, and oversight / monitoring arrangements support informed risk taking. Levels of fraud controls are varied to reflect scale of risk with costs.
Operations	Defensive approach to operational delivery - aim to maintain/protect, rather than create or innovate. Priority for close management controls and oversight with limited devolved authority.	Innovations largely avoided unless essential. Decision making authority held by senior management.	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Management through leading indicators.	Innovation supported, with clear demonstration of benefit / improvement in management control. Responsibility for non-critical decisions may be devolved.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust / lagging indicators rather than close control.
Legal	Play safe and avoid anything which could be challenged, even unsuccessfully.	Want to be very sure we would win any challenge.	Want to be reasonably sure we would win any challenge.	Challenge will be problematic; we are likely to win, and the gain will outweigh the adverse impact.	Chances of losing are high but exceptional benefits could be realised.
Property	Obligation to comply with strict policies for purchase, rental, disposal, construction, and refurbishment that ensures producing good value for money.	Recommendation to follow strict policies for purchase, rental, disposal, construction, and refurbishment that ensures producing good value for money.	Requirement to adopt arrange of agreed solutions for purchase, rental, disposal, construction, and refurbishment that ensures producing good value for money.	Consider benefits of agreed solutions for purchase, rental, disposal, construction, and refurbishment that meeting organisational requirements.	Application of dynamic solutions for purchase, rental, disposal, construction, and refurbishment that ensures meeting organisational requirements.
Financial	Avoidance of any financial impact or loss, is a key objective.	Only prepared to accept the possibility of very limited financial impact if essential to delivery.	Seek safe delivery options with little residual financial loss only if it could yield upside opportunities.	Prepared to invest for benefit and to minimise the possibility of financial loss by managing the risks to tolerable levels.	Prepared to invest for best possible benefit and accept possibility of financial loss (controls must be in place).
Commercial	Zero appetite for untested commercial agreements. Priority for close management controls and oversight with limited devolved authority.	Appetite for risk taking limited to low scale procurement activity. Decision making authority held by senior management.	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Management through leading indicators.	Innovation supported, with demonstration of benefit / improvement in service delivery. Responsibility for non-critical decisions may be devolved.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust / lagging indicators rather than close control.
People	Priority to maintain close management control & oversight. Limited devolved authority. Limited flexibility in relation to working practices. Development investment in standard practices only	Decision making authority held by senior management. Development investment generally in standard practices.	Seek safe and standard people policy. Decision making authority generally held by senior management.	Prepared to invest in our people to create innovative mix of skills environment. Responsibility for noncritical decisions may be devolved.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust rather than close control.

Risk appetite level definitions					
	Averse	**Minimal**	**Cautious**	**Open**	**Eager**
Technology	General avoidance of systems / technology developments.	Only essential systems / technology developments to protect current operations.	Consideration given to adoption of established / mature systems and technology improvements. Agile principles are considered.	Systems / technology developments considered to enable improved delivery. Agile principles may be followed.	New technologies viewed as a key enabler of operational delivery. Agile principles are embraced.
Data & Info Management	Lock down data & information. Access tightly controlled, high levels of monitoring.	Minimise level of risk due to potential damage from disclosure.	Accept need for operational effectiveness with risk mitigated through careful management limiting distribution.	Accept need for operational effectiveness in distribution and information sharing.	Level of controls minimised with data and information openly shared.
Security	No tolerance for security risks causing loss or damage to HMG property, assets, information or people. Stringent measures in place, including: • Adherence to FCDO travel restrictions • Staff vetting maintained at highest appropriate level. • Controls limiting staff and visitor access to information, assets and estate. • Access to staff personal devices restricted in official sites	Risk of loss or damage to HMG property, assets, information or people minimised through stringent security measures, including: • Adherence to FCDO travel restrictions • All staff vetted levels defined by role requirements. • Controls limiting staff and visitor access to information, assets and estate. • Staff personal devices permitted, but may not be used for official tasks.	Limited security risks accepted to support business need, with appropriate checks and balances in place: • Adherence to FCDO travel restrictions • Vetting levels may flex within teams, as required • Controls managing staff and limiting visitor access to information, assets and estate. • Staff personal devices may be used for limited official tasks with appropriate permissions.	Considered security risk accepted to support business need, with appropriate checks and balances in place: • New starters may commence employment at risk, following partial completion of vetting processes • Permission may be sought for travel within FCDO restricted areas. • Controls limiting visitor access to information, assets and estate. • Staff personal devices may be used for official tasks with appropriate permissions.	Organisational willing to accept security risk to support business need, with appropriate checks and balances in place: • New starters may commence employment at risk, following partial completion of vetting processes • Travel permitted within FCDO restricted areas. • Controls limiting visitor access to information, assets and estate. • Staff personal devices permitted for official tasks
Project/Programme	Defensive approach to transformational activity - aim to maintain/protect, rather than create or innovate. Priority for close management controls and oversight with limited devolved authority. Benefits led plans fully aligned with strategic priorities, functional standards.	Innovations avoided unless essential. Decision making authority held by senior management. Benefits led plans aligned with strategic priorities, functional standards.	Tendency to stick to the status quo, innovations generally avoided unless necessary. Decision making authority generally held by senior management. Plans aligned with strategic priorities, functional standards.	Innovation supported, with demonstration of commensurate improvements in management control. Responsibility for noncritical decisions may be devolved. Plans aligned with functional standards and organisational governance.	Innovation pursued – desire to 'break the mould' and challenge current working practices. High levels of devolved authority – management by trust rather than close control. Plans aligned with organisational governance.
Reputational	Zero appetite for any decisions with high chance of repercussion for organisations' reputation.	Appetite for risk taking limited to those events where there is no chance of any significant repercussion for the organisation.	Appetite for risk taking limited to those events where there is little chance of any significant repercussion for the organisation.	Appetite to take decisions with potential to expose organisation to additional scrutiny, but only where appropriate steps are taken to minimise exposure.	Appetite to take decisions which are likely to bring additional Governmental / organisational scrutiny only where potential benefits outweigh risks.

II. Orange Book example risk categories

The Orange Book recommends risks should be organised by taxonomies or categories of risk. Grouping risks in this way supports the development of an integrated and holistic view of risks. Annex 4 of the Orange Book provides the following example categories. These are not intended to be exhaustive. Failure to manage risks in any of these categories may lead to financial, reputational, legal, regulatory, safety, security, environmental, employee, customer and operational consequences.

Strategy risks – Risks arising from identifying and pursuing a strategy, which is poorly defined, is based on flawed or inaccurate data or fails to support the delivery of commitments, plans or objectives due to a changing macro-environment (e.g. political, economic, social, technological, environment and legislative change).

Governance risks – Risks arising from unclear plans, priorities, authorities and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance.

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).

Property risks – Risks arising from property deficiencies or poorly designed or ineffective/ inefficient safety management resulting in non-compliance and/or harm and suffering to employees, contractors, service users or the public.

Financial risks – Risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting.

Commercial risks – Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, and /or failure to meet business requirements/objectives.

People risks – Risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviours, the unavailability of sufficient capacity and capability,

industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance.

Technology risks – Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.

Information risks – Risks arising from a failure to produce robust, suitable and appropriate data/information and to exploit data/information to its full potential.

Security risks – Risks arising from a failure to prevent unauthorised and/or inappropriate access to key government systems and assets, including people, platforms, information and resources. This encompasses the subset of cyber security.

Project/Programme risks – Risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost and quality.

Reputational risks – Risks arising from adverse events, including ethical violations, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damages to reputation and or destruction of trust and relations.

III. Example risk appetite descriptions

The following example demonstrates how risk appetite statements may guide organisational activity and decision making.

A. Example organisational appetite summary

Our risk appetite has been defined following consideration of organisational risks, issues and consequences. Appetite levels will vary, in some areas our risk tolerance will be **cautious** in others, we are **open/hungry** for risk and are willing to carry risk in the pursuit of important objectives. We will always aim to operate organisational activities at the levels defined below. Where activities are projected to exceed the defined levels, this must be highlighted through appropriate governance mechanisms.

- **Reputational risks:** We have adopted a **cautious** stance for reputational risks, with a preference for safer delivery options, tolerating a cautious degree of residual risk and choosing the option most likely to result in successful delivery, thereby enhancing our reputation for delivering high quality, cost-effective services to the public.
- **Financial risks:** We have adopted a **cautious** stance for financial risks with reference to core running costs, seeking safe delivery options with little residual risk that only yield some upside opportunities. The Board will receive ongoing assurance through the annual governance statement that policies and procedures are in place in line with HMT guidance.
- **Information risks**: We have adopted a varied stance to information risk, to reflect the sensitivity of information as defined by Government Security Classifications (GSC). The Board will receive an annual assurance that guidance and procedures are in place and training undertaken by staff.
  - Tier 1 (Official/Official Sensitive): We have adopted an **open** stance, given the need for operational effectiveness with risk mitigated through careful drafting and/or limiting distribution;
  - Tier 2 (Secret): We have adopted a **minimal** stance to limit the potential damage from disclosure;
  - Tier 3 (Top Secret): We have adopted an **averse** stance where disclosure would lead to serious risks to national security, economic well-being, or widespread loss of life.
- **Personnel security risks**: We have adopted a **cautious** stance for personnel security risks, and a **cautious** stance for security risks to staff. This includes both staff within the UK and those travelling and based abroad. The Board will receive an annual assurance that appropriate travel advice and briefings are undertaken, and vetting, procedures and duty of care is in place.
- **Cyber risks:** We have adopted a **cautious** stance for cyber risks. The Board will have independent assurance, on service entry and in-life, on the risk of fraud and inadvertent or malicious corruption or modification of data on its IT systems.
- **Assets/Estates risks:** We have adopted **cautious** and **open** stances for assets and estates respectively, seeking value for money but with a preference for proven delivery options that have a cautious residual risk. This means that we use solutions for purchase, rental, disposal, construction, and refurbishment that ensure we protect the taxpayer from as much risk as possible, producing good value for money whilst fully meeting organisational requirements.

- **Business continuity risks**: We have adopted a **cautious** stance for incident management and business continuity risks. The Board will receive ongoing assurance from annual testing of business continuity plans.
- **Legal/Regulatory compliance risks**: We have adopted a **cautious** stance for compliance, seeking a preference for adhering to responsibilities, and safe delivery options with little residual risk. The Board will have annual assurance that compliance regimes are in place.

B. Example detailed thematic statement

Financial: The organisation's appetite for financial risk is operating within the risk tolerance position: **cautious.**

Our financial decisions are heavily scrutinised, with value for money being a key factor in decision making. We will accept risks that may result in some small-scale financial loss or exposure on the basis that these can be expected to balance out but will not accept financial risks that could result in significant reprioritisation of budgets. Our appetite for risks associated with business as usual activity is naturally lower than with our transformation activity. Within this our risk appetite is:

- **Averse** for financial propriety and regularity risks with a determined focus to maintain effective financial control framework accountability structures.
- **Averse** in terms of risks related to our qualification of accounts, associated process and deviation from reporting timetables.
- **Minimal** as to risk relating to breaching individual control totals.
- **Cautious** for risks related to our business partnering model.
- **Open** in relation to our budget spend with the intention that we should maximise the use of resource each year. We are prepared to over-programme by £Xm at the start of each year with this amount being actively monitored and managed, if necessary, to ensure it reduces at each quarter during the year.

IV. Risk appetite scales

The risk appetite scale examples provided below are based on successful practice collated from the Civil Service Risk Community

Example 1

Risk Appetite	Description
Opposed	Avoidance of risk and uncertainty is key objective
Minimalist	Preference for safe options that have a low degree of inherent risk
Cautious	Preference for safe options that have a low degree of residual risk
Mindful	Willing to consider all options and choose one that is most likely to result in successful delivery
Enterprise	Eager to be innovative and to choose options that suspend previous held assumptions and accept greater uncertainty

Example 2

Risk Appetite	Description
Averse	Avoidance of risk and uncertainty in achievement of key deliverables or initiatives is key objective. Activities undertaken will only be those considered to carry virtually no inherent risk.
Minimalist	Preference for very safe business delivery options that have a low degree of inherent risk with the potential for benefit/return not a key driver. Activities will only be undertaken where they have a low degree of inherent risk.
Cautious	Preference for safe options that have low degree of inherent risk and only limited potential for benefit. Willing to tolerate a degree of risk in selecting which activities to undertake to achieve key deliverables or initiatives, where we have identified scope to achieve significant benefit and/or realise an opportunity. Activities undertaken may carry a high degree of inherent risk that is deemed controllable to a large extent.
Open	Willing to consider all options and choose one most likely to result in successful delivery while providing an acceptable level of benefit. Seek to achieve a balance between a high likelihood of successful delivery and a high degree of benefit and value for money. Activities themselves may potentially carry, or contribute to, a high degree of residual risk.
Eager	Eager to be innovative and to choose options based on maximising opportunities and potential higher benefit even if those activities carry a very high residual risk.

Annex B: Acknowledgements

The Government Finance Function extends thanks to colleagues from the following organisations who were instrumental in compiling this guide.

ALARM
embrace risk

CPS

Department for Education

Department for Environment Food & Rural Affairs

Department for International Trade

Department for Transport

Department for Work & Pensions

Foreign, Commonwealth & Development Office

Government Internal Audit Agency

Government Security Group

METROPOLITAN POLICE

Ministry of Defence

Ministry of Housing, Communities & Local Government

Ministry of Justice

TRANSPORT FOR LONDON

UKAD

This page is left blank

Produced by Mark Ripley, Government Finance Function