RISK MANAGEMENT STRATEGY

Version	6
Date of approval by SMT	22 February 2022
Date of Previous approval	1 February 2020 15 June 2017 8 October 2014 29 September 2010 3 March 2016
Date of next Review	February 2023

Contents

1. Introduction and Purpose

1.1. The Commission is primarily concerned with the achievement of Outcomes. The organisation exists for a purpose. Whatever the purpose, the efficient, effective and economic delivery of services and achievement of desired outcomes will face all manner of ***risks***.

1.2. The task of management is to respond to these risks so as to maximise the likelihood of achieving the purpose. The resources available for doing so are finite and so the aim is to achieve an optimum ***response to risk***, prioritised in accordance with an evaluation of the risks. Some degree of risk taking is necessary – the only way to avoid risk is to do nothing at all, but all this will do is guarantee nothing will be achieved. Managers therefore need to be equipped with the skills and tools that allow them to have a reasonable assurance of achieving their outcomes and delivering value for money.

1.3. The essence of risk is the uncertainty of a particular outcome (whether positive or negative). The term '***exposure*** to risk' refers to the combination of the ***Likelihood*** (probability) of potential events occurring and the magnitude of their ***Impact***.

- ***Likelihood***: the evaluated probability of a particular risk actually happening (including a consideration of the frequency)
- ***Impact***: the evaluated effect or result of a particular risk actually happening.

The task of ***Risk Management*** is the management of this exposure to risk to an acceptable level, by taking action on likelihood and/or impact: it therefore requires identification of the elements to be considered - not all of which may be controllable.

1.4. Risk can be thought of as arising in two ways:

- direct ***threats*** (damaging events) which could lead to failure to achieve outcomes: and
- ***opportunities*** (constructive events), which, if exploited, could offer an improved way of achieving outcomes but which are surrounded by threats.

In either case the Commission needs to put in place a corporate and consistent strategy for managing risk in order to ensure that it has an agreed and understood methodology for achieving its outcomes.

1.5. As with business planning and performance monitoring, the Commission needs to be able to handle risk at all levels, strategic, operational and project level. At the strategic level, what is at stake is the Commission's contract with the Department and its stakeholders. Decisions will involve the formulation of strategic outcomes and the resource allocation decisions to support them. At the operational and project level, decisions are made on procurement, establishing projects, business continuity, resource management, managing schedules, managing providers and partners.

1.6. Figure 2 – Risk management in practice: roles and responsibilities from the NIAO Publication "Good practice in risk management", June 2011, provides an overview of how Risk Management should be handled in an organisation;

Accounting Officer	• Retains ultimate responsibility for the organisation's system of internal control and ensures that an effective risk management process is in place and is regularly reviewed • Provides clear direction to staff • Establishes, promotes and embeds an organisational risk culture • Reports to the Board and the Audit Committee
Board	• Establishes and oversees risk management procedures • Endorses the risk management strategy/policies • Ensures appropriate monitoring and management of significant risks by management • Challenges risk management to ensure that all key risks have been identified • Is aware of any instances where risks are realised
Audit & Risk Assurance Committee	• Reports to the Board on the effectiveness of the system of internal control and alerts the Board members to any emerging issues • Endorses the organisation's risk management strategy/policies • Takes responsibility for the oversight of the risk management process • Reviews risk registers to provide challenge and advice (not in an executive capacity)
Senior Management	• Acts on behalf of the Board and will: ➢ determine the organisation's approach to risk management ➢ implement policies on risk management and internal control ➢ discuss and approve issues that significantly affect the organistion's risk profile or exposure ➢ continually monitor the identification and management of significant risks and ensure that actions to remedy control weakness are implemented ➢ report changes in risk assessment to the Board on an exception basis ➢ annually review the organisation's approach to risk management and approve changes or improvements to key elements of its processes and procedures ➢ report to the Audit Committee and to the Board on risk management matters • Provides subsidiary management/internal control statements to the Accounting Officer
Risk Owner	• Identifies and assesses individual risks • Decides whether a risk is sufficiently serious to be escalated to the next level of the organisation • Ensures that actions to treat or control the risk are carried out and informs the risk manager of any consequent updates to the risk register • Reviews the risk rating and the necessity to keep the risk on the register

Risk Management Function e.g. risk champion/ manager/co-ordinator/ department	• Maintains the risk register under the direction of risk owners and updates or amends the risk register as necessary • Regularly reviews the content of risk registers with a view to ensuring that risk actions are being completed and that all details on the risk register are correct
Staff	• Carry out risk actions identified and delegated by the risk owners • Maintains awareness of the organisation's risk management strategy and the key risks faced by the organisation • Ensures that duties relating to controls are carried out
Internal Audit	• Provides independent opinion on the overall adequacy and effectiveness of the organisation's framework of governance, risk management and internal control to the Accounting Officer (and Audit Committee)

1.7. The objective of risk management in the Commission is to ensure that our threats and opportunities are managed effectively thereby creating, as far as possible, an environment of 'No Surprises'. By managing risks effectively we will be in a stronger position to deliver a high quality service and better value for money for the taxpayers i.e. achieve our business outcomes.

1.8. When our management of risk goes well it often passes unnoticed. When it fails, the consequences can be significant and high profile. We all want to avoid this – hence the need for effective risk management.

1.9. A Risk Management Strategy is an essential element of strategic planning. This Risk Management Strategy describes the processes that need to be in place to identify, evaluate, address, monitor and report on our risks and describes the principles that underpin the Commission's approach to risk management.

1.10. Risk management will only become standard practice if there is a better understanding of what it involves and the benefits that it brings in terms of helping to achieve business outcomes. We need to take a proactive approach to ensure that less time is spent reacting to situations and more time is spent taking advantage of opportunities.

1.11. Four key principles underpin the Risk Management Strategy:

- Transparency
- Co-ordination
- Public credibility
- Effectiveness

1.12. ***Transparency*****:** We will be open in our approach to managing risks and will not attribute blame. Staff, external organisations and members of the public should expect to have access to information on our current risks and how we are managing them. The risk information we provide should help managers and individuals to take appropriate action themselves.

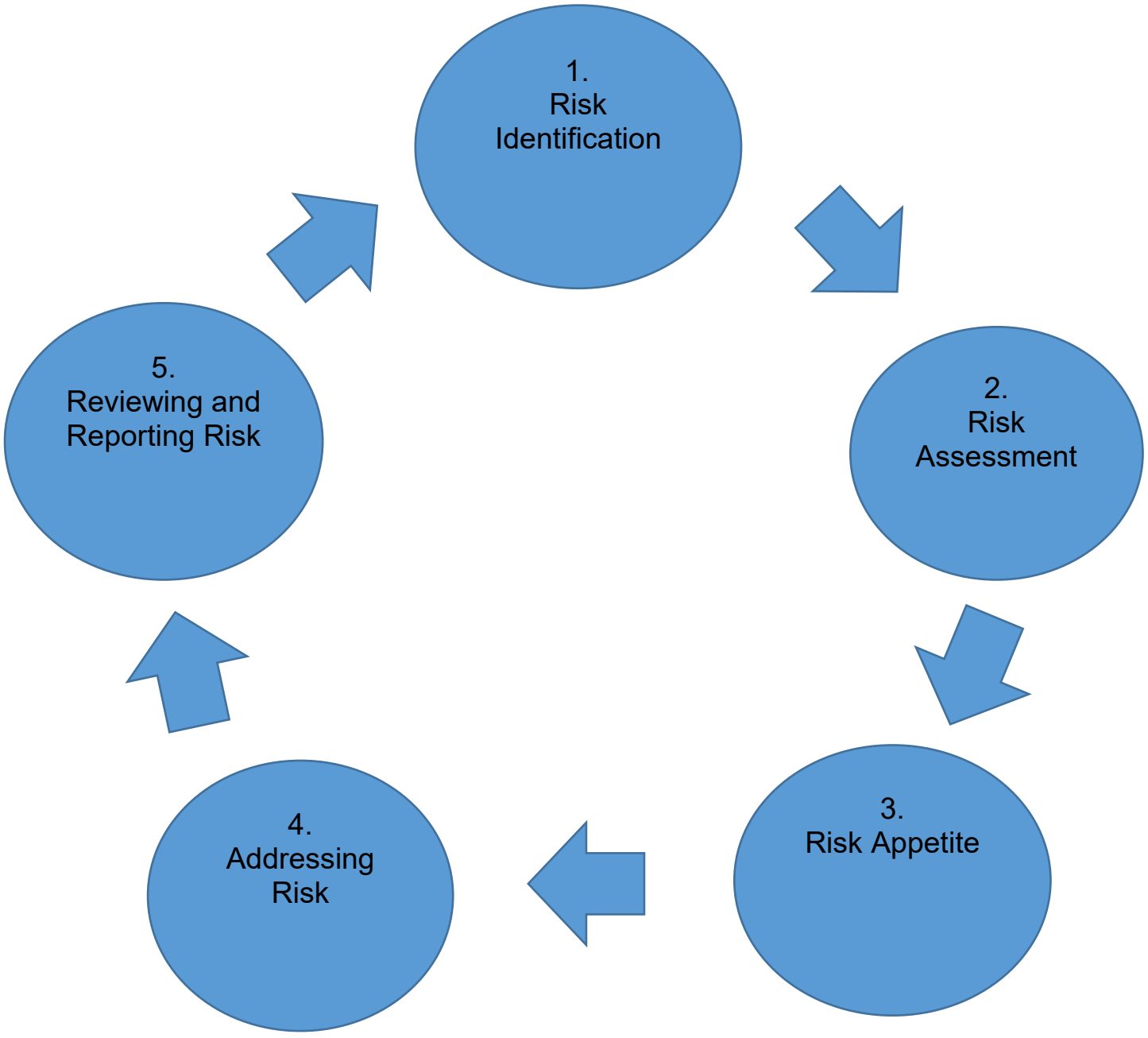
1.13. ***Co-ordination:*** We will be consistent in how we evaluate and manage our risks throughout the Commission. We will work closely with others to share best practice and learn.

1.14. ***Public Credibility:*** We will seek to gain the trust and confidence of our stakeholders in all that we do and operate at the highest levels of corporate governance.

1.15. ***Effectiveness:*** We will adopt a robust approach to risk management – aiming to identify, evaluate, address, review and report on risk in a way that can stand audit scrutiny, building on best practice and protecting the interests of our stakeholders. We will be accountable by laying our processes and data open to review by the Northern Ireland Audit Office and our own Internal Auditors and we will respond to any improvements they suggest.

2. The Risk Management Process

2.1. Figure 3 – The Risk Management Process from the NIAO Publication "Good practice in risk management", June 2011, provides visual illustration of the process;



There is a continuous 'cycle' to the risk management process. Whilst each of the steps in the process can follow each other it should be noted that all of them should also be undertaken continuously and together. The Risk Management Process should not have a beginning and an ending, but Risk Assessment and the processes which follow should be undertaken on an ongoing and continuous basis.

3. Identifying Risks

3.1. Our approach to risk management will be objective driven. The Commission's Vision, Aims and Outcomes have been agreed at Ministerial level and these now drive the critical aspects of the Commission's activities. For example, how we plan our business and allocate resources, how we create and revise our workplan and how we measure and review our performance.

3.2. A risk is something that may have an impact on the achievement of our outcomes. It may come from outside the Commission (e.g. the impact of the political climate) or from inside (e.g. lack of resources). It may include information risks when the information used to support our business decisions is incomplete, out-of-date or inaccurate. It may also be the risk that the information we hold could become lost, stolen or destroyed.

3.3. The table below outlines the main types of risk that we are likely to encounter in our work situation, though it is not intended to be exhaustive. It provides a starting point for staff seeking to identify potential risks in their areas of work.

3.4. Risks need to be assessed in terms of how likely they are and the magnitude of the consequences if they were to occur. The modern view of business risk and one that Commission wants to encourage in is that some risks are opportunities to be embraced, not just threats to be avoided.

Types of Risk

External Risk	Risks from a change in the economic or political climate or changing public attitudes.
Financial Risk	Risks arising from internal and external fraud or impropriety; from failed resource bids or insufficient resources.
Operational Risk	Risks associated with recruitment difficulties or diversion of staff to other duties; risks surrounding IT systems; risks associated with the provision of facilities and equipment; risks associated with incomplete, out-of-date or inaccurate information as well as the loss or theft of information.
Project Risk	Risks of overspending or overrunning compared with budgets and forecasts on capital projects, or risks associated with insufficient forward planning or horizon scanning.
Reputational Risk	Risks from damage to the Commission's credibility and reputation.
Shared Risks	Risks from joined-up working or change programmes, or risks experienced by our partners or suppliers that would have a knock-on impact on the Commission's Outcomes.
Strategic Risk	Risks arising from policy decisions or organisational changes; risks arising from senior-level decisions on priorities. Includes the risk of failing to meet government standards or laws and regulations when giving advice.

3.5. We will support our identification of risks through good systems for gathering intelligence (management information systems).

3.6. When risks have been identified essential information about them will be recorded in the form of a ***Risk Register.*** Team and Corporate Risk Registers will be maintained and reviewed on a monthly basis.

3.7. We recognise that the identification of risks is an ongoing task. We believe that a culture that systematically identifies risks should be well placed to assess and address its risks. It should also be well placed to identify opportunities, and we plan to be in this position – bringing improved performance through the calculated taking of opportunities.

4. Assessing and Rating Risks

4.1. Our goal is to be effective risk managers. To do this we will need to be good at assessing those risks that we have identified. This is a difficult area and one that calls for a consistent approach.

Risk Appetite

4.2. One of the essential elements of the process is to agree the Commission's Risk Appetite. Risk Appetite is defined in the Orange Book[1] as 'the amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time'. This level of risk is considered in terms of the opportunities, threats and costs, it should be noted that it is not considered in terms of costs alone.

4.3. An example of behaviours we consider when making our assessment is appended at **Annex 1**. This Annex provides a table outlining some typical behaviour we need to consider when assessing risk appetite.

4.4. Risk Appetite can be classified in the following way.

Classification	Description
Averse	Avoidance of risk and uncertainty is a key Organisational objective.
Minimalist	Preference for ultra-safe business delivery options that have a low degree of inherent risk and only have limited potential for reward.
Cautious	Preference for safe delivery options that have a low degree of residual risk and may have only limited potential for reward.
Open	Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward (and value for money etc…
Hungry	Eager to be innovative and to choose options offering potentially higher business rewards, despite greater inherent risk.

4.5. The Commission has assigned a Risk Appetite to each of its Corporate Outcomes based on assessment using the criteria above. These have been approved by the Commission's Board.

Corporate Outcome	Risk Appetite
1. Improved health and wellbeing of victims and survivors	Cautious / Open

[1] Orange Book: Management of Risk – Principles and concepts: Available from HM Treasury Website

2. Victims and survivors, and those most in need, are helped and cared for	Cautious / Open
3. Victims and survivors, and their families, are supported to engage in legacy issues	Cautious / Open
4. Children and grandchildren of victims and survivors are given the best start in life	Cautious / Open
5. Improved access to opportunities for learning and development for victims and survivors.	Cautious / Open
6. We are an effective and efficient organisation	Averse

Mechanism for escalating Risks

4.6. Risks should be identified within each Commission Unit (Communications and Engagement; Research and Policy Development; and Corporate Services) and recorded on the individual Unit Risk Registers.

4.7. At each SMT meeting the Unit Heads should present a statement of assurance which details how they accept responsibility for maintaining a robust system of internal control and support the achievement of the Commission's policies, aims and objectives. This statement should also detail that the Unit Head has assessed the risk and control mechanisms in their area of responsibility, should provide assurance to the Accounting Officer that the Risk Management framework is in place, and detail any exceptions.

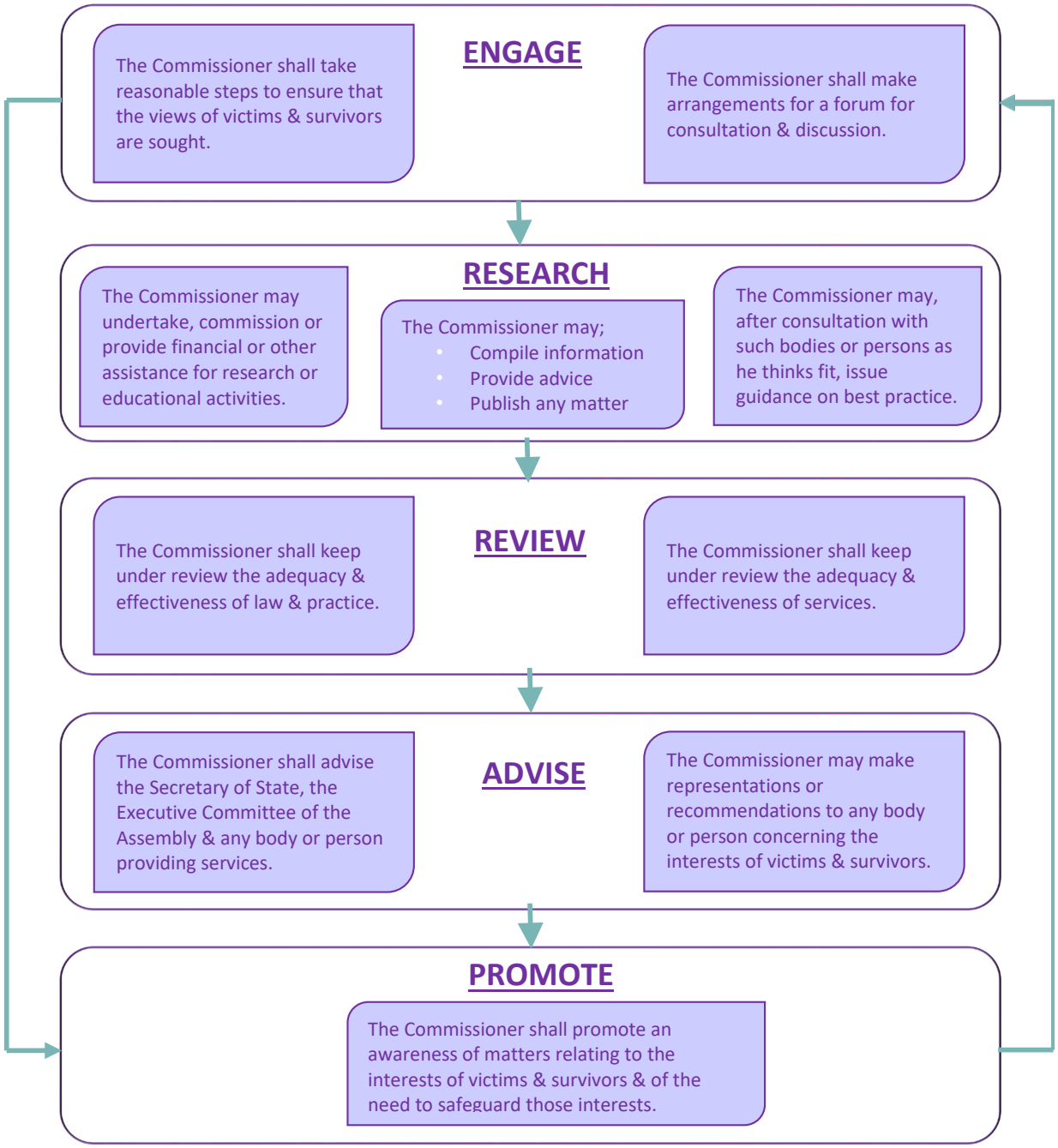
4.8. These exceptions will be recorded on the Corporate Risk Register.

Mechanism for requesting change to agreed Risk Appetite

4.9. Any risks which emerge outside the Commission's Risk Appetite (i.e **"?"**) should be notified to the Secretary to the Commission by the relevant person without delay. These risks will be discussed and agreed by SMT, and will be recorded in the Corporate Risk Register as appropriate.

4.10. The Corporate Risk Register is reviewed at SMT meetings, at Board on a monthly basis and by the Audit & Risk Assurance Committee on a quarterly basis.

Assessing Risks



4.11. This flow diagram illustrates how the Commission performs its core functions and meets its statutory duties. It also highlights the inter-dependency in managing risks from the outset at initial engagement stage.

4.12. Consideration is given to whether the risks identified in the Corporate Risk Register are at a level which the Commission can accept, or if other mitigating actions need to be taken into account.

4.13. To assess risks adequately we need to identify the ***consequences*** of a risk materialising and give each risk a ***risk rating.***

4.14. Assessment Inherent is the Risk Assessment before any controls have been put in place. Assessment Residual is after the Controls in Place have been actioned. The Risk Register also takes account of the external dependencies affecting the work of the Commission. Therefore inherent risk is high across a number of the Statutory functions, however the Commission cannot accept full responsibility for certain risk areas and has reflected this in the assessment of residual risk.

Consequences

4.15. Given the types of risk that Commission will encounter, the consequences of those risks can be grouped into one or more of the following categories:

- *Operational* (e.g. targets missed)
- *Legal* (e.g. claims against the Commission)
- *Reputational* (e.g. loss of public confidence)

4.16. Using these categories will allow us to group similar risks and to begin the process of identifying potential crosscutting risks. We will also use this as an aid to identifying appropriate risk owners.

Risk Rating ~ Programme and Project (Operational) Levels

4.17. We need to have some means of comparing our risks so that we can concentrate our efforts on addressing those that are the most important. We will use an approach which gives each risk a relative rating i.e. ***Likelihood*** and its ***Impact***

4.18. The Likelihood of the risk arising should be defined (in accordance with HMT Guidance) in terms of:

- High – more likely to occur than not
- Medium – fairly likely to occur
- Low – unlikely to occur

4.19. Similarly the assessed Impact of the risk should be defined as:

- High
- Medium
- Low

4.14. These ratings will be displayed in the Commissions Risk Register in a 3 x 3 matrix as below;

Likelihood	Impact		
	Low 1	Medium 2	High 3
High 3			
Medium 2			
Low 1			

Actions to Improve Control

4.15. If the existing controls in place are determined not to be adequate or acceptable then appropriate Actions to Improve Controls should be entered and the criticality of each rated as:

- High
- Medium
- Low

5. Addressing Risks

5.1. When responding to a risk, our goal will be to ensure that it does not develop into an issue. To do this we will build on HM Treasury's guidance in their 'Orange Book'. Having properly identified and assessed our risks, we will select one of the following general approaches (the Four Ts):

- *Transfer the risk*: This might be done through such things as conventional insurance or by asking a third party to take on the risk in another way.
- *Tolerate the risk*: Our ability to take effective action against some risks may be limited, or the cost of taking action may be disproportionate to the potential benefit gained. In this instance, the only management action required is to 'monitor' the risk to ensure that its likelihood or impact does not change. If new management options arise, it may become necessary to treat the risk in the future.
- *Treat the risk*: by far the greater number of risks will be in this category. The purpose of treatment is not necessarily to terminate the risk but, more likely, to set in train a planned series of mitigating actions to contain the risk to an acceptable level; and
- *Terminate the risk*: this is a variation of the 'treat' approach and involves quick and decisive action to eliminate a risk altogether. For example, the health or environmental impacts of using a particular chemical may be such that the appropriate action is to ban it. The introduction of new technology may also remove certain existing risks though it will often result in a new set to be addressed.

5.2. In addressing risks, we will seek to adopt a proportionate response – reducing risks to 'as low a level as is reasonably practicable' in the particular circumstances. In deciding on the preferred course of action, we will consider the use of a range of available risk management tools and techniques, including options appraisal, and will implement Guidelines 2000, which sets out the Government's key principles applying to the development and presentation of scientific advice for policy making.

5.3. The Commissions Risk Register will also provide detail of the assessment of the Risk and the resulting Residual Risk.

Contingencies

5.4. We recognise that any risks could suddenly be realised and become a critical issue, even those assessed as having a relatively low Likelihood. Our assessments could be wrong, circumstances might change before we have time to respond or external events could alter our view of situations and the nature of the risk. We will consider in advance what action to take if a risk develops or a crisis occurs. These are our '***Contingency Plans***' and they are essential to creating an environment of 'No Surprises'.

5.5. We will prepare a ***Business Continuity Plan*** to help keep the organisation running during times of change or disruption. These will usually be for relatively isolated events, such as office moves or organisational change and will be the responsibility of the manager of the relevant business area affected.

7. Reviewing and Reporting Risks

6.1. The HM Treasury guidance "Assurance Frameworks" (December 2012) advises;

"The Accounting Officer, supported by the Board, is responsible for ensuring that there are robust governance, risk management and internal control arrangements across the whole organisation, including any sponsored bodies. Authority, in terms of accountability and respective delegations, needs to be appropriately and clearly established and monitored. This responsibility includes the Accounting Officer demonstrating...that he/she has maintained a sound system of risk management and internal control in stewardship of the organisation's resources, which is affirmed in his/her signature of the Governance Statement."

6.2. Appropriate and effective review and reporting arrangements will enforce and support our risk management activities. This will allow up-to-date and accurate performance information to be passed to risk owners and senior managers along with information on other performance measures.

6.3. Risk management is a dynamic and ongoing process – new risks will be identified, some will be terminated, contingency plans and countermeasures will need to be updated in response to changing internal and external events, and our assessment of likelihood and impact will also need to be reviewed, particularly in the light of our own management actions.

6.4. The Board, as advised by the Audit & Risk Assurance Committee, will keep the main risks under regular strategic review. The HM Treasury guidance "Assurance Frameworks" (December 2012) advises;

"Whilst the Board will most closely monitor its key risks, it will otherwise delegate the monitoring of assurance to the Audit and Risk Committee (ARC), or appropriate equivalent body in the organisation, made up of independent Non Executive Directors. This is not a substitute for management's responsibility for the mitigation of risks. On behalf of the Board, the ARC will examine the arrangements in place to provide comprehensive and reliable assurance. This involves identifying the assurance need, how it will be met, whether there are any assurance gaps or overlaps, how these can best be filled and whether this will provide the sufficient, relevant, reliable assurance that it needs. These arrangements should be monitored throughout the year to ensure that sufficient assurance is being planned and delivered to avoid surprises and to enable early decisions and action to be taken on risk and control issues. This will help to routinely validate assurance. A good framework is required to support the governance process.

There are different types of assurance that may have different strengths and may be best used in different ways. The Audit and Risk Committee can therefore play a key role in seeking an optimum mix of assurance."

6.5. The HM Treasury guidance "Assurance Frameworks" (December 2012) suggests a Three Lines of Defence model for an assurance framework which has been adopted by the Commission;

6.6. The First Line is within the business operational areas, and arrangements are established that can be used to provide assurance on how well outcomes are being met and risks managed. This includes good policy and performance data, monitoring the risk register, the provision of exception reports and other management information. For example, the Risk Register will presented to the Board quarterly with significant risk issues, or changes from the last review, highlighted.

6.7. The Second Line is associated with oversight of management activity and although separate from those responsible for delivery, it is not independent of the organisation's management chain. It includes compliance assessments or reviews carried out to determine that policy or quality arrangements are being met in line with expectations for specific areas of risk across the organisation. This could be a review of information security or the delivery of key strategic outcomes.

6.8. The Third Line relates to independent and more objective assurance. It focuses on the role of internal audit and places reliance upon assurance mechanisms in the first and second lines of defence, where possible, to enable it to direct its resources most effectively, on areas of highest risk or gaps or weaknesses.

6.9. As an additional line of assurance, sitting outside of the Three Lines of Defence model, are external auditors, the NIAO, who have a statutory responsibility for certification audit of the financial statements.

6.10. The Accounting Officer and the Board will need to ensure that they are receiving sufficient and timely assurance information on the management of risk to enable them to exercise good oversight. This will include reports from the Audit and Risk Assurance Committee, review from Internal Audit, feedback from staff, reporting at various levels of the organisation (SMT and Board) and effective programme and project management, with similar and proportionate oversight and assurance reporting arrangements in place to manage and monitor services outsourced to external suppliers.