

# Revenue Scotland

## Risk Management Framework

<b>1. Introduction .....</b>	<b>2</b>
1.2 <b>Overview of risk management .....</b>	<b>2</b>
<b>2. Policy Statement .....</b>	<b>3</b>
<b>3. Risk Management Approach .....</b>	<b>4</b>
3.1 <b>Risk management objectives .....</b>	<b>4</b>
3.2 <b>Risk management vision .....</b>	<b>4</b>
3.3 <b>Risk management culture .....</b>	<b>4</b>
3.4 <b>Risk management structure .....</b>	<b>5</b>
3.5 <b>Responsibilities .....</b>	<b>5</b>
3.6 <b>Risk registers .....</b>	<b>6</b>
<b>4. Risk Management Process .....</b>	<b>6</b>
4.2 <b>Risk identification .....</b>	<b>6</b>
4.3 <b>Analysing and assessing risk .....</b>	<b>7</b>
4.4 <b>Responding to and managing risk .....</b>	<b>10</b>
4.5 <b>Monitoring and control arrangements .....</b>	<b>11</b>
12	
4.7 <b>Learning .....</b>	<b>13</b>
<b>Annex 1 - Responsibilities for Risk Management .....</b>	<b>14</b>
<b>Annex 2 - Risk Impact Descriptions .....</b>	<b>17</b>
<b>Appendix 5 - Risk Maturity Model .....</b>	<b>22</b>

## 1. Introduction

1.1 This document sets out Revenue Scotland's approach to risk management and outlines the key objectives, strategies and responsibilities for the management of risk across the organisation. It applies to all Revenue Scotland staff and should be applied consistently across the organisation. It will be supported by training to ensure that staff are risk “aware”.

### 1.2 Overview of risk management

1.2.1 Revenue Scotland is committed to achieving its aims as defined in the Corporate Plan and Business Plan. In doing so, Revenue Scotland recognises that it will face a variety of risks.

1.2.2 Risk is defined as a quantifiable level of exposure to the threat of an event or action that will adversely affect Revenue Scotland's ability to achieve its objectives successfully. The task of management is to respond to these risks effectively so as to maximise the likelihood of Revenue Scotland achieving its objectives and ensuring the best use of resources.

1.2.3 We use risk management to systematically identify, record, monitor and report risks to enable the organisation to meet its objectives and to plan actions to mitigate those risks. There are six key elements of Revenue Scotland's risk management process as illustrated in Diagram 1 below:

**Diagram 1: Revenue Scotland's Risk Management Process**



## 2. Policy Statement

- 2.1 Revenue Scotland is committed to ensuring that the management of risk underpins all business activities of the organisation and that thorough risk management procedures are in place throughout the organisation.
- 2.2 The application of this Framework will enable Revenue Scotland to obtain, maintain and respond to a changing risk profile.
- 2.3 Revenue Scotland has a responsibility to manage risks (both positive and negative) and to support a systematic approach to risk management including the promotion of a risk aware culture. This requires risks to be regularly identified, reviewed and updated.
- 2.4 The application of risk management practices should not and will not eliminate all risk exposure. Moreover, through the application of the risk management approach identified in this Framework we aim to achieve a better understanding of the risks faced by Revenue Scotland and their implications for the business, thus informing decision-making.
- 2.5 Revenue Scotland recognises that risk, as well as posing a threat, also represents opportunities for developing innovative ways of working. Innovation and best practice should be shared across Revenue Scotland.
- 2.6 The identification and management of risks affecting Revenue Scotland's ability to achieve its objectives is set out in the Corporate Plan and other supporting documentation such as the Business Plan and the Corporate Risk Register.
- 2.7 Revenue Scotland expects management to take action to avoid or, where appropriate, mitigate the effects of those risks that are considered to exceed Revenue Scotland's risk appetite. Where a risk is deemed to exceed Revenue Scotland's risk appetite it will be captured in the corporate risk register along with the actions being taken to mitigate the risk.
- 2.8 The active, on-going commitment and full support of the Revenue Scotland Board through the work of the Audit and Risk Committee and Revenue Scotland Senior Management Team is an essential part of this Risk Management Framework. The Chief Executive and senior management team will ensure that effective mechanisms are in place for assessing, monitoring and responding to any risks arising, whilst the Board retain ultimate responsibility for overseeing the Framework.
- 2.9 All employees are expected to have an understanding of the nature of risk within Revenue Scotland and of the organisation's risk appetite. Where Revenue Scotland has delegated functions to other bodies, the risks associated with carrying out those functions will lie with the delegate body except where alternative arrangements, e.g. for financial risks, are set out in the relevant Memorandum of Understanding. It is the responsibility of the Revenue Scotland Senior Management Team to raise on the Corporate Risk Register any significant risks having an impact on other bodies that could affect delivery of Revenue Scotland's purpose and objectives.

### **3. Risk Management Approach**

#### **3.1 Risk management objectives**

3.1.1 To assist in the management of business and organisational risk the following objectives have been identified. These form the basis of Revenue Scotland's Risk Management Strategy:-

- Promote awareness of business and organisational risk and embed the approach to its management throughout the organisation.
- Seek through appropriate assessment criteria to identify, measure, control and report on any business and organisational risks that have the potential to undermine the achievement of Revenue Scotland's business priorities, either strategic or operational.

#### **3.2 Risk management vision**

3.2.1 Revenue Scotland will aim to identify risks and their causes at the earliest opportunity; measure the risk effect on the organisation; and put in place controls to mitigate risks.

3.2.2 Additionally, Revenue Scotland will seek to obtain assurance that the controls relied on to mitigate the key risks are effective. An assurance framework has been developed to support the on-going monitoring of controls (see under “monitoring and control”).

#### **3.3 Risk management culture**

3.3.1 Revenue Scotland recognises the value of a strong risk management culture for maintaining an excellent service to taxpayers and the confidentiality of protected taxpayer information. Consequently, it will:

- review the Corporate Plan on an annual basis;
- review the corporate risk register on a quarterly basis;
- integrate risk management with planning and delivery;
- implement and monitor risk management arrangements across the organisation;
- oversee appropriate delegation of responsibility for risk ownership and management;
- ensure that designated individuals receive the necessary training, on-going support and advice on risk management; and
- measure progress in its approach to risk management.

### 3.4 Risk management structure

3.4.1 To ensure that Revenue Scotland has a full understanding of the risks being faced and the implications for the organisation, risks will be identified and assessed at three levels:-

**Corporate:** those business risks that, if realised, could have a significant detrimental effect on Revenue Scotland's key business processes and activities, including reputational and financial risks.

**Operational:** those business risks that, if realised, could have a significant detrimental effect on the key operational objectives and activities.

**Project/ Programme:** those business risks that, if realised, could have a significant detrimental effect on the outcome of a programme or project.

### 3.5 Responsibilities

3.5.1 The Revenue Scotland Board, through the Audit and Risk Committee, has ultimate responsibility for the management of risk, whereas the Revenue Scotland Senior Management Team has day to day responsibility for the system of internal control including risk management.

3.5.2 All staff should be risk aware. The key roles and responsibilities in relation to risk are summarised at **Annex 1** to this document.

**Diagram 2 describes where ownership and assurance of registers lies:**



### 3.6 Risk registers

3.6.1 The corporate and programme/ project risk registers will follow a standard format, set out at **paragraphs 4.5.3** and **4.5.4** below and at **Annexes 3** and **4**, including the following elements:-

- gross risk assessments of likelihood and impact;
- controls in place, both current and proposed, to mitigate the gross risks;
- current risk assessments of likelihood and impact;
- target risk scores;
- risk proximity, i.e. the time period in which the risk is likely to occur.

**Corporate Risk Register:** This register reflects the most significant risks that have the potential for Revenue Scotland to fail to meet its objectives as detailed in the Corporate Plan. Revenue Scotland's Senior Management Team maintain and update the Corporate Risk Register.

**Operational Registers:** The operational teams may maintain their own risk registers which reflect the specific risks associated with their activities.

**Programme / Project Risk Registers:** A separate risk register must be maintained for each major programme and project. Any significant risks should be evaluated to decide whether they merit inclusion in the corporate risk register.

## 4. Risk Management Process

### 4.1. Revenue Scotland's risk management process

- identify the risks inherent in our strategic and operating environment;
- analyse, assess and rank the risks (according to residual, or current, risk);
- address the risks by implementing controls to manage the risks;
- respond to and manage the risks;
- monitor and review the effectiveness of the management process and the controls;
- learn from the management of individual risks and continually improve the overall management of risk.

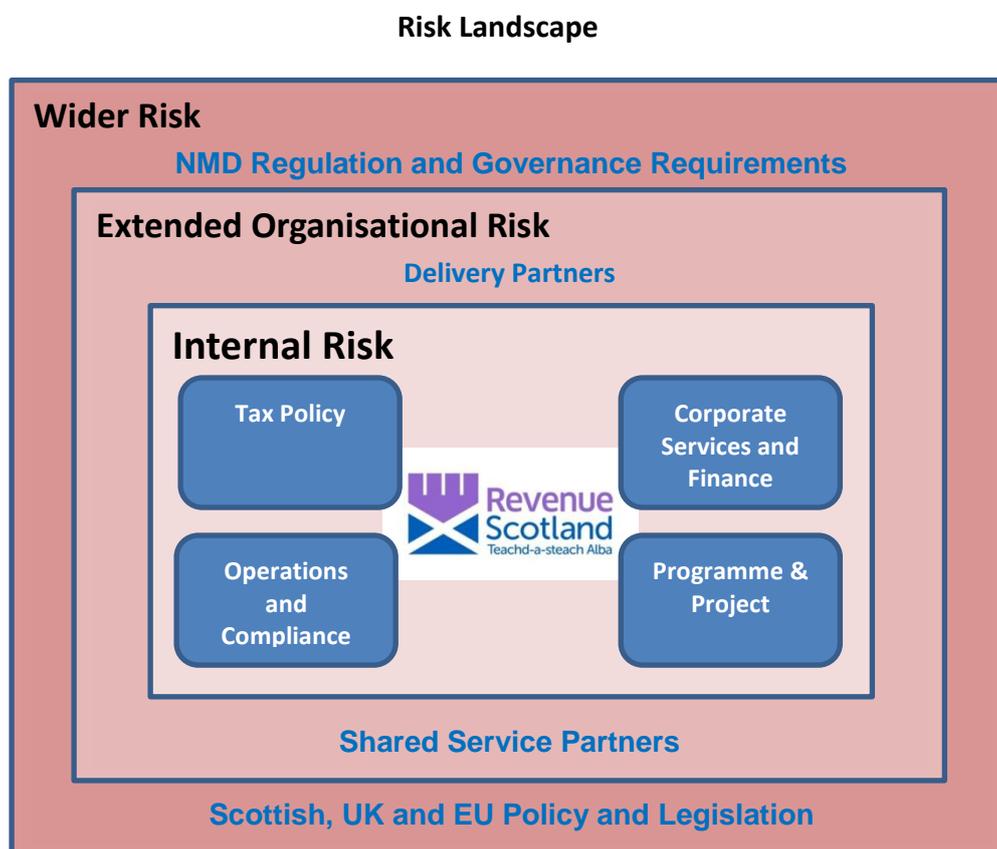
### 4.2 Risk identification

4.2.1 Risk identification is an on-going activity, with individual risks and the impact and/or likelihood of risk changing frequently. Risk identification is the process of determining what objectives you are seeking to achieve and identifying what can threaten the achievement of these objectives.

4.2.2 Risks can be identified from a number of sources including: internal and external audit activities; management scrutiny and discussion; working groups; team meetings; information from the media / publications; horizon scanning; recurring and on-going complaints; and changing legislation. It is important, therefore, that risk features as a **standard agenda item** on all team

meetings and working groups across Revenue Scotland. Any risks identified should be reported for inclusion in the relevant risk register.

4.2.3 **Diagram 3 - Risk Landscape** provides a view of the levels of risk which could have an impact on Revenue Scotland:



### 4.3 Analysing and assessing risk

4.3.1 Once a risk is identified, it needs to be assessed. Risks should be assessed consistently across Revenue Scotland considering – the **likelihood** of the risk occurring, and if the risk were to occur, what the **impact (i.e. consequences)** on the organisation would be.

4.3.2 Likelihood will be categorised on a scale of 1 to 5 with one being *rare* and five *highly likely*. Impact will also be assessed on a scale of 1 to 5 with one being *negligible* and 5 being *catastrophic*. Likelihood and impact are multiplied together to obtain a total gross risk score, as illustrated in **Diagram 4**:

**Diagram 4: Risk Scoring**

## Risk Management Matrix

<b>Likelihood</b>	<b>Highly likely (5)</b>	5	10	15	20	25
	<b>Probable (4)</b>	4	8	12	16	20
	<b>Occasional (3)</b>	3	6	9	12	15
	<b>Unlikely (2)</b>	2	4	6	8	10
	<b>Rare (1)</b>	1	2	3	4	5
		<b>Negligible (1)</b>	<b>Minor (2)</b>	<b>Serious (3)</b>	<b>Major (4)</b>	<b>Catastrophic (5)</b>
		<b>Impact</b>				

4.3.3 A table setting out what is meant by *Negligible*, *Minor*, *Serious*, *Major* and *Catastrophic*, classified by various types of events, is included at **Annex 2**.

### **Risk proximity**

4.3.4 A third element that needs to be considered when assessing risk is its proximity, which is the time period in which the risk is likely to occur. Understanding the proximity will help us to choose and prioritise mitigating actions. The following four levels of proximity are used in the Risk Management Framework:-

- 1) 0 - 3 Months
- 2) 3 - 6 Months
- 3) 6 - 9 Months
- 4) 9 Months +

## Risk appetite

4.3.5 Risk appetite is an expression of how much risk Revenue Scotland is prepared to accept. Those involved in risk evaluation and prioritisation should, when considering risk, discuss and express the risk appetite as they see it.

4.3.6 The risk register prompts risk owners to consider risk appetite when updating a risk entry. They need to consider not only the risk score before and after existing mitigating action but also the final tolerable risk status (i.e. what they are aiming for in terms of status for that particular risk).

4.3.7 Revenue Scotland's risk appetite can be summarised as follows:

**Table 1: Risk Appetite**

Risk Rating	Net risk assessment	Risk appetite response
<b>Black</b>	<b>25</b>	Unacceptable level of risk exposure which requires action to be taken urgently.
<b>Red</b>	<b>16 - 20</b>	'Red risks' at Operational / Project level should be included in the corporate risk register and activity to reduce the risk immediately undertaken.
<b>Amber</b>	<b>10 - 15</b>	Acceptable level of risk, in the short term, but one which requires action and active monitoring to ensure risk exposure is reduced.
<b>Yellow</b>	<b>5 - 9</b>	Acceptable level of risk but one which requires consideration of action and active monitoring to reduce risk exposure.
<b>Green</b>	<b>1 - 4</b>	Acceptable level of risk based on the operation of normal controls. In some cases it may be acceptable for no mitigating action to be taken e.g. net risk < 4.

#### 4.4 Responding to and managing risk

4.4.1 Based on risk scores there are four options available to address risk, as follows:

**Terminate** - In this situation the risk is terminated by deciding not to proceed with the activity. For example, if a particular project is very high risk and the risk cannot be mitigated it might be decided to cancel the project. Alternatively, the decision may be made to carry out the activity in a different way.

**Transfer** - In this scenario, another party bears or shares all or part of the risk. For example, this could include transferring out an area of work or using insurance.

**Treat** - This involves identifying mitigating actions or controls to reduce risk. These controls should be monitored on a regular basis to ensure that they are effective.

**Tolerate** - In this case, it may not always be necessary (or appropriate) to take action to treat risks, for example, where the cost of treating the risk is considered to outweigh the potential benefits. If the risk is shown as 'green' after existing mitigating actions, then it can probably be tolerated.

##### Mitigating actions

4.4.2 These are the controls put in place within Revenue Scotland to reduce the likelihood of occurrence of the risk or to minimise the impact of the risk if it does occur: an internal control system incorporating policies, processes, business continuity arrangements and other aspects of Revenue Scotland's operations that, taken together:

- enable the organisation to respond appropriately to business and organisational risks;
- help ensure the quality of internal and external reporting. This requires the maintenance of proper records and processes that generate the flow of timely, relevant and reliable information; and
- help ensure compliance with applicable laws and regulations, and also with internal policies. This would include, for example, having formal written procedures and policies applied consistently across the organisation, supported by training for staff.

4.4.3 The risk that remains after taking account of the relevant mitigations is referred to as the current risk.

##### Risk escalation

4.4.4 This is a method of internal communication which ensures that significant risk information is passed upwards to an appropriate person or group. This is necessary to ensure that the appropriate decisions and/or actions are implemented to mitigate the risk.

4.4.5 It is key to the risk escalation process that the right information is made available at the right management level at the right time. There is no restriction on what may be escalated for action. However, the key criterion is that intervention is required from higher management.

4.4.6 It is the responsibility of individual risk owners to raise risks which they believe require action by a higher authority. However, it should be remembered that the overarching principle for the escalation of risks requiring action is: If in doubt, escalate.

4.4.7 Risks should feature as a standard agenda item at all management and working group meetings. Risks should be discussed, evaluated and escalated, as appropriate, to ensure that the most significant risks (and mitigating actions) are reflected in the corporate risk register.

#### 4.5 **Monitoring and control arrangements**

##### **Monitoring and Reviewing risks**

4.5.1 Risk management is an on-going process that needs to be embedded in everyday activity. The process must be reviewed on a regular basis to remain effective. It is the responsibility, therefore, of each risk owner to review risks on a regular basis and to identify whether any revisions are required. The revision may involve a re-assessment of impact and likelihood or planned mitigating actions.

4.5.2 As previously stated, it is important that risk is included as a standing item on the agenda for management teams (at all levels within the organisation) and working groups so that risks can be identified and captured.

4.5.3 Each risk should have a **Risk Profile Card** completed by the risk owner for input on the risk register. A Word template is provided at **Annex 3**.

4.5.4 A **Risk Summary** should be drawn up for each Risk Profile Card completed, and updated every quarter or as required to show (a) movement in the impact/ likelihood assessment of the risk and (b) any significant action(s) taken since the previous update. A Word template is provided at **Annex 4**.

4.5.5 An Assurance Framework has been developed to ensure that risk management is used as a management tool contributing to the success of Revenue Scotland. Detailed roles and responsibilities are covered at **Annex 1**. The diagram below sets out who carries out checks, and when. Internal Audit will also look at risk as part of their on-going reviews and in identifying future audits.

#### 4.6 Reporting



4.6.1 Revenue Scotland's risk management framework will be supported through agreed reporting and assurance arrangements. This is to ensure that the key risks and their owners are clearly identified, that mitigation and specified actions are appropriate and that actions are being carried out. The arrangements include the following:

##### Corporate level

4.6.2 The Revenue Scotland Board will review and approve risk management policies and strategies, and determine the risk appetite and the risk management process maturity. It will take advice from the Audit and Risk Committee on these matters. The Audit and Risk Committee will scrutinise the Corporate Risk Register at each quarterly meeting and the Board will do so at least twice annually.

4.6.3 On a routine basis the Audit and Risk Committee will receive updates on Revenue Scotland's risk management framework and on corporate risks. Reporting will include:-

- Revenue Scotland's approach to risk appetite;
- the Risk Management Framework and Revenue Scotland's approach to risk;
- the Corporate Risk Register including associated action plans for higher rated risks; and
- reports on the changing risk profile within Revenue Scotland including areas of increasing risk, areas where controls are not considered to be effective, and horizon scanning for areas of possible future risk.

4.6.4 The Audit and Risk Committee will also review the corporate risk register at each meeting and will receive an annual report on risk from the internal Auditors. The Committee will also consider input from other sources of assurance as may be appropriate.

4.6.5 The Audit and Risk Committee will submit an annual written report to the Revenue Scotland Board which includes an appropriately updated version of the Corporate Risk Register.

4.6.6 The Revenue Scotland Senior Management Team will maintain and regularly review (and update) the corporate risk register of the key risks facing the organisation.

#### **Operational Level**

4.6.7 Heads of Service and those to whom they have delegated a lead role in risk management will review risks and actions in mitigation of risks on a regular basis as an integral part of the business planning process. They will also ensure that risks identified at an operational level and which may have a wider impact on the organisation are escalated as appropriate.

#### **Programme/ Project level**

4.6.8 Risks associated with Programmes and projects will be reviewed by the project sponsor or officer responsible for maintaining the project risk register depending on delegated authority. Risks identified in project risk registers which may have a wider impact on the organisation should be escalated.

### **4.7 Learning**

#### **Risk Management Maturity**

4.7.1 A key aspect of monitoring and reporting progress is the establishment of a Risk Maturity Model. This provides senior management with a snapshot of where the risk principles and processes that Revenue Scotland employs have led to changes and progression in risk management. It provides assurance that risk management processes are fit for purpose and also identifies areas where further improvement is required. Revenue Scotland's risk maturity model is attached as **Annex 5**. The risk maturity model will be reviewed annually by the Revenue Scotland Senior Management Team who will report findings and any actions to raise "maturity" in areas of poorer performance to the Audit and Risk Committee and for subsequent approval by the Board.

## Annex 1 - Responsibilities for Risk Management

Level	Role & responsibilities	Frequency of activity
<b>Revenue Scotland Board</b>	Overall ownership of risk	On-going
	Setting the tone for risk management throughout the organisation	On-going
	Approving the overall risk management arrangements including the Risk Management Framework and the appetite for risk	Annually
	Considering reports on the operation of risk management arrangements from the Audit and Risk Committee and the Accountable Officer and through consideration of the annual assurances for the completion of the annual report and accounts.	Annually
	Reviewing the Corporate Risk Register	At least twice annually
<b>Audit and Risk Committee</b>	Scrutinising Revenue Scotland's Risk Management Framework and ensuring it is kept under review and updated	Annually
	Reviewing the strategic processes for risk, control and governance (including the Accountable Officer's Governance Statement)	Annually
	Monitoring the effectiveness of risk management arrangements	Quarterly
	Scrutinising Revenue Scotland's approach to risk tolerance (i.e. risk appetite)	Annually
	Reviewing the corporate risk register	Each Meeting
	Escalating to the Board issues that pose a material risk to the delivery of Revenue Scotland's aims, strategic objectives and major programmes	Each Meeting
	Escalating to the Board any other areas of concern	Each Meeting

Level	Role & responsibilities	Frequency of activity
<b>Accountable Officer</b>	Specific personal responsibility for signing the annual accounts including the Accountable Officer's Governance Statement.	Annually
	Responsible for reporting on risk management to the Board	Each Board Meeting
<b>Revenue Scotland Senior Management Team</b>	Responsible for implementing the Risk Management Framework within their areas of responsibility and accountability	On-going
	Owners of the corporate risk register and responsible for ensuring its completeness and accuracy	On-going
	Approving and recommending the draft Risk Management Framework to the Audit and Risk Committee	Annually
	Ensuring that every significant risk is owned by a member of the Senior Management Team	On-going
	Reviewing and challenging 'red' (high) risks	On-going
	Escalating all appropriate risks to the Corporate Risk Register	On-going
	Reviewing corporate risks including approach (Terminate/Transfer/Tolerate /Treat)	On-going
	Preparing corporate business plan incorporating risks and planned mitigating actions	Annually
	Reviewing risk maturity	Annually
	Fostering a culture of risk management and risk awareness	On-going
	Ensuring that all identified risks are captured in the relevant risk register	On-going
	Actively managing risks through identification of mitigating controls, taking action and regularly discussing and reporting on risks	On-going

Level	Role & responsibilities	Frequency of activity
	Risk being a standing item on meetings held by senior management with their teams.	On-going
<b>Other staff</b>		
<b>Risk Owner</b> (the designated individual to manage and monitor risks. For corporate risks included in corporate risk register).	Maintaining all aspects of risk assigned to the risk owner, including ensuring that controls and actions needed to mitigate the risk are in place and an action plan is maintained	Monthly
	Obtaining senior management support where necessary	On-going
	Escalating risks where appropriate	On-going
<b>All Staff</b>	Following Revenue Scotland's risk management framework	On-going
	Understanding risk and being aware of the role of risk owners	On-going
	Having a good understanding of the part they play in delivering Revenue Scotland's risk management framework	On-going
	Being risk aware and reporting potential risks to line management for consideration.	On-going
	Determining opportunities from risk management for innovative ways of working	On-going

## Annex 2 - Risk Impact Descriptions

Impact Rating	Financial Risk Guide	Human Risk Guide	Asset Risk Guide	Timing risk guide	Reputational Risk Guide	Scope Risk Guide	Reputational Risk Guide
<b>Negligible</b>	<£5k of expenditure	Minor injury, or illness, first aid, no days lost	Minor damage to single asset	<0.5 days	Minor media interest	<2.5% variance	Act or Omission resulting in Legal or Regulatory breach causing insignificant impact loss (as categorised in other six impact categories)
<b>Minor</b>	£5k to £30k of expenditure	Minor injury, or illness, medical treatment, days lost	Minor damage to multiple assets	0.5 to 1 day	Headline media interest	2.5-5% variance	As above Causing minor loss including possibly minor loss of tax revenue
<b>Serious</b>	£30k to £150k of expenditure	Moderate injury, medical treatment, hospitalisation, <14 days lost, RIDDOR reportable	Major damage to single or multiple assets	1 to 7 days	Headline media interest causing public embarrassment	5-10% variance	As above Causing moderate loss including possibly moderate loss of tax revenue
<b>Major</b>	£150k to £0.5m of expenditure	Single death, extensive injuries, long-term illness (>14 days)	Significant loss of assets	7 to 30 days	Short-term media campaign	10-25% variance	As above Causing major loss including major loss of tax revenue

<b>Impact Rating</b>	<b>Financial Risk Guide</b>	<b>Human Risk Guide</b>	<b>Asset Risk Guide</b>	<b>Timing risk guide</b>	<b>Reputational Risk Guide</b>	<b>Scope Risk Guide</b>	<b>Reputational Risk Guide</b>
<b>Catastrophic</b>	>£0.5m of expenditure	Multiple deaths or severe disabilities	Complete loss of assets	>30 days	Sustained media campaign or lobbying	>25% variance	As above Causing catastrophic loss, including possibly catastrophic loss of tax revenue and Legal or regulatory supervision

Risk Profile Card		[Reference Number in Bold]																																																																								
<u>Objective</u> .	<u>Source of objective</u>																																																																									
<u>Risk</u> <b>[Title in Bold]</b>	<u>Date risk identified</u>																																																																									
<u>Risk owner</u>	<u>Date risk profile card last reviewed</u>																																																																									
<u>How would this risk happen?</u> • .	<u>What would the potential outcome be?</u> •																																																																									
<u>What early warning indicators would let us know the risk was likely to happen?</u> •	<u>What information are managers receiving to let them know how well risk is being managed?</u> •																																																																									
<u>Existing controls to manage risk</u> •	<u>Additional controls needed to manage this risk</u> •																																																																									
<p><b>Current risk assessment</b></p> <table border="1"> <tr><td>5</td><td>Yellow</td><td>Orange</td><td>Orange</td><td>Red</td><td>Grey</td></tr> <tr><td>4</td><td>Green</td><td>Yellow</td><td>Orange</td><td>Red</td><td>Red</td></tr> <tr><td>3</td><td>Green</td><td>Yellow</td><td>Yellow</td><td>Orange</td><td>Orange</td></tr> <tr><td>2</td><td>Green</td><td>Green</td><td>Yellow</td><td>Yellow</td><td>Orange</td></tr> <tr><td>1</td><td>Green</td><td>Green</td><td>Green</td><td>Green</td><td>Yellow</td></tr> <tr><td></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr> </table> <p>Likelihood</p> <p>Impact</p>	5	Yellow	Orange	Orange	Red	Grey	4	Green	Yellow	Orange	Red	Red	3	Green	Yellow	Yellow	Orange	Orange	2	Green	Green	Yellow	Yellow	Orange	1	Green	Green	Green	Green	Yellow		1	2	3	4	5	<p>Risk Movement since previous assessment</p> <table border="1"> <tr><td>↑</td><td></td></tr> <tr><td>↔</td><td></td></tr> <tr><td>↓</td><td></td></tr> </table>		↑		↔		↓																															
5	Yellow	Orange	Orange	Red	Grey																																																																					
4	Green	Yellow	Orange	Red	Red																																																																					
3	Green	Yellow	Yellow	Orange	Orange																																																																					
2	Green	Green	Yellow	Yellow	Orange																																																																					
1	Green	Green	Green	Green	Yellow																																																																					
	1	2	3	4	5																																																																					
↑																																																																										
↔																																																																										
↓																																																																										
<p><b>Initial risk assessment</b></p> <table border="1"> <tr><td>5</td><td>Yellow</td><td>Orange</td><td>Orange</td><td>Red</td><td>Grey</td></tr> <tr><td>4</td><td>Green</td><td>Yellow</td><td>Orange</td><td>Red</td><td>Red</td></tr> <tr><td>3</td><td>Green</td><td>Yellow</td><td>Yellow</td><td>Orange</td><td>Orange</td></tr> <tr><td>2</td><td>Green</td><td>Green</td><td>Yellow</td><td>Yellow</td><td>Orange</td></tr> <tr><td>1</td><td>Green</td><td>Green</td><td>Green</td><td>Green</td><td>Yellow</td></tr> <tr><td></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr> </table> <p>Likelihood</p> <p>Impact</p>	5	Yellow	Orange	Orange	Red	Grey	4	Green	Yellow	Orange	Red	Red	3	Green	Yellow	Yellow	Orange	Orange	2	Green	Green	Yellow	Yellow	Orange	1	Green	Green	Green	Green	Yellow		1	2	3	4	5	<p><b>Target risk assessment</b></p> <table border="1"> <tr><td>5</td><td>Yellow</td><td>Orange</td><td>Orange</td><td>Red</td><td>Grey</td></tr> <tr><td>4</td><td>Green</td><td>Yellow</td><td>Orange</td><td>Red</td><td>Red</td></tr> <tr><td>3</td><td>Green</td><td>Yellow</td><td>Yellow</td><td>Orange</td><td>Orange</td></tr> <tr><td>2</td><td>Green</td><td>Green</td><td>Yellow</td><td>Yellow</td><td>Orange</td></tr> <tr><td>1</td><td>Green</td><td>Green</td><td>Green</td><td>Green</td><td>Yellow</td></tr> <tr><td></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr> </table> <p>Likelihood</p> <p>Impact</p>		5	Yellow	Orange	Orange	Red	Grey	4	Green	Yellow	Orange	Red	Red	3	Green	Yellow	Yellow	Orange	Orange	2	Green	Green	Yellow	Yellow	Orange	1	Green	Green	Green	Green	Yellow		1	2	3	4	5
5	Yellow	Orange	Orange	Red	Grey																																																																					
4	Green	Yellow	Orange	Red	Red																																																																					
3	Green	Yellow	Yellow	Orange	Orange																																																																					
2	Green	Green	Yellow	Yellow	Orange																																																																					
1	Green	Green	Green	Green	Yellow																																																																					
	1	2	3	4	5																																																																					
5	Yellow	Orange	Orange	Red	Grey																																																																					
4	Green	Yellow	Orange	Red	Red																																																																					
3	Green	Yellow	Yellow	Orange	Orange																																																																					
2	Green	Green	Yellow	Yellow	Orange																																																																					
1	Green	Green	Green	Green	Yellow																																																																					
	1	2	3	4	5																																																																					
Risk proximity at initial assessment: (1) 0-3 months; (2) 4-6 months; (3) 7-9 months; (4) 9 months +																																																																										

<b>Risk Profile Card</b>		<b>[Reference Number in Bold]</b>	
Action to be taken		<u>Name of body / person deciding action to be taken</u> (programme board / management team)	
Tolerate		<u>Date decision taken</u>	
Treat			
Transfer			
Terminate			
Take the opportunity			
Overall target date to reduce this risk to the target level			
Proposed actions to put additional controls in place and/or other actions to manage this risk			
	Action	Action owner	Delivery date
1			
2			
3			
4			

Corporate Risk Register Summary Card – at [insert date]

<b>Risk Number</b>						
<b>Risk</b>						
<b>Date Opened</b>						
<b>Owner</b>						
	<b>Initial risk score</b>	<b>I</b>	<b>L</b>	<b>Score</b>	<b>Date created</b>	
<b>Risk scores</b>	<b>Previous score</b>	<b>risk</b>	<b>I</b>	<b>L</b>	<b>Score</b>	<b>Date assessed</b>
	<b>Current score</b>	<b>risk</b>	<b>I</b>	<b>L</b>	<b>Score</b>	<b>Date assessed</b>
	<b>Target score</b>	<b>risk</b>	<b>I</b>	<b>L</b>	<b>Score</b>	<b>Planned achievement date</b>
<b>Current risk proximity</b>						
<b>Update</b>						

## Appendix 5 - Risk Maturity Model

	Risk Governance	Risk identification & assessment	Risk mitigation & treatment	Risk reporting & review	Continuous improvement
<b>Enabled</b>	Risk management and internal control is fully embedded into operations. All parties play their part and have a share of accountability for managing risk in line with their responsibility for the achievement of objectives.	There are processes for identifying and assessing risks and opportunities on a continuous basis. Risks are assessed to ensure consensus about the appropriate level of control, monitoring and reporting to carry out. Risk information is documented in a risk register.	Responses to the risks have been selected and implemented. There are processes for evaluation risks and responses implemented. The level of residual risk after applying mitigating controls is accepted by the organisation, or further mitigations have been planned.	High quality, accurate and timely information is available to operational management and directors. The board reviews the risk management strategy, policy and approach on a regular basis, e.g. annually, and review key risks, emergent & new risks, and action plans on a regular basis.	The organisational performance management framework and reward structure drives improvements in risk management. Risk management is a management competency. Management assurance is provided on the effectiveness of their risk management on a regular basis.
<b>Managed</b>	Risk management objectives are defined and managers are trained in risk management techniques. Risk management is written into performance expectations of managers. Management	There are clear links between objectives and risks at all levels. Risk information is documented in a risk register. The organisation's risk appetite is used in the scoring system for assessing risks. All	There is clarity on the risk level that is accepted within the organisation's risk appetite. Risk responses are appropriate to satisfy the risk appetite of the organisation have been selected and implemented.	The Board reviews key risks, emergent and new risks, and action plans on a regular basis. It reviews the risk management framework, policy and approach on a regular basis (annually). Senior managers require interim updates from delegated	The organisation's risk management approach and the Board's risk appetite are regularly reviewed and refined in light of new risk information reported. Management assurance is provided on the effectiveness of their

	Risk Governance	Risk identification & assessment	Risk mitigation & treatment	Risk reporting & review	Continuous improvement
	and executive level of responsibilities for key risks have been allocated.	significant projects are routinely assessed for risk.		managers on individual risks for which they have personal responsibility.	risk management on an ad hoc basis. The resources used in risk management are cost effective. Measures are set to improve certain aspects of risk management activity e.g. number of risks materialising or surpassing impact – likelihood expectations.
<b>Defined</b>	A risk management framework and policies are in place and communicated. The level of risk taking that the organisation will accept is defined and understood in some parts of the organisation, and it is used to consider the most appropriate responses to the management of	There are processes for identifying and assessing risks and opportunities in some parts of the organisation but not consistently applied in all. All risks identified have been assessed with a defined scoring system. Risk information is brought together for some parts of the organisation. Most projects are assessed for	Management in some parts of the organisation are familiar with, and able to distinguish between, the different options available in responding to risks to select the best response in the interest of the organisation.	Management have set up methods to monitor the proper operation of key processes, responses, and actions plans. Management report risks to Heads of Service where responses have not managed the risks to a level acceptable to the Board.	The Board gets minimal assurance on the effectiveness of risk management.

	Risk Governance	Risk identification & assessment	Risk mitigation & treatment	Risk reporting & review	Continuous improvement
	identified risks. Management and executive level of responsibilities for key risks have been allocated.	risk.			
<b>Aware</b>	There is a scattered, silo-based approach to risk management. The vision, commitment and ownership of risk management have been documented. However, the organisation is reliant on a few people for the knowledge, skills and practice of risk management activities on a day-to-day basis.	A limited number of managers are trained in risk management techniques. There are processes for identifying and assessing risks and opportunities, but these are not fully comprehensive or implemented. There is no consistent scoring system for assessing risks. Risk information is not fully documented.	Some responses to the risks have been selected and implemented by management according to their own perception of risk appetite in the absence of a Board-approved appetite for risk.	There are some monitoring processes and ad hoc reviews by some managers on risk management activities.	Management does not assure the Board on the effectiveness of risk management.
<b>Naive</b>	No formal approach developed for risk management. No	Processes for identifying and evaluating risks and responses are not	Responses to the risks have not been designed or implemented.	There are no monitoring processes or regular reviews of risk	Management does not assure the Board on the effectiveness of risk

	<b>Risk Governance</b>	<b>Risk identification &amp; assessment</b>	<b>Risk mitigation &amp; treatment</b>	<b>Risk reporting &amp; review</b>	<b>Continuous improvement</b>
	formal consideration of risks to business objectives, or clear ownership, accountability and responsibility for the management of key risks.	defined. Risks have not been identified or collated. There is no consistent scoring system for assessing risks.		management.	management.

