DRAFT

Risk Management Framework

Version: 0_1 November 2021
Owner: Corporate Performance Team
Approved by:

Risk Management Framework - DRAFT

1. Introduction

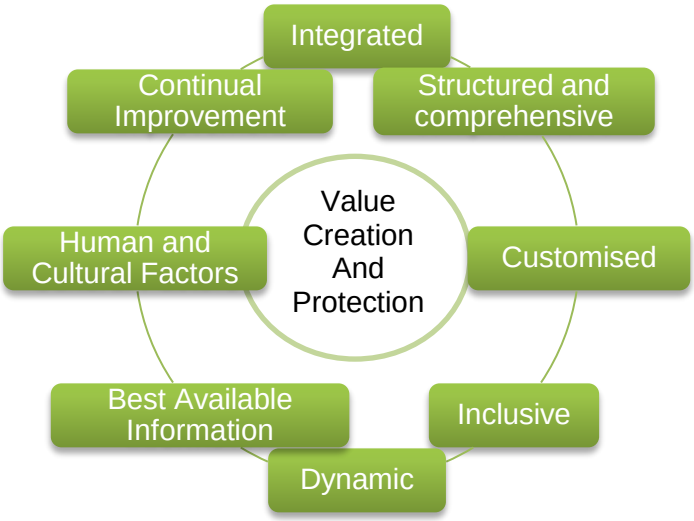
This document sets out our rules and standards for managing strategic and operational risks and guides staff in assessing, monitoring and managing risk on a day-to-day basis. It applies to all risks identified across the organisation.

2. Principles of risk management

2.1 There are 8 principles of risk management, shown in the graphic below, which are the foundation for managing risk, which have been considered when establishing the organisations' risk management framework and processes. These principles enable us to manage the effects of uncertainty on its objectives.

2.2 The international standard for risk management (ISO 31000) sets out useful guidance on risk management, emphasising that it should be integral to all processes and for all staff. Good principles for managing risk are that:

- It needs to be systematic, structured and timely.
- It is based on the best available information, including historical data, stakeholder and customer feedback, forecasting and expert judgement. It should be tailored to the organisation's internal and external context and risk profile.
- It takes human and cultural factors into account, recognising that people's capabilities, behaviours and intentions can either help or hinder the organisation's objectives.
- It is transparent and inclusive, needing the timely and appropriate involvement of stakeholders and decision makers at each stage, ensuring proper representation of all those affected.
- It needs to be iterative, dynamic and responsive to change, taking account of changes in the internal and external environment.
- It needs to demonstrate continuous improvement.



3. Defining risk

3.1 In this context, “risk” refers to an uncertain event, or set of events, which may affect our ability to operate its business or achieve its aims and objectives. An “uncertain event” is one that might happen, rather than one that will definitely happen or is happening already.

3.2 Each risk has the key dimensions of “likelihood” and “impact”. Likelihood is the probability the event will happen, while impact is the impact the event would have if it happened.

4. Managing Risk

4.1 We must be able to consider the risks that may threaten or affect the running of its business and delivery of its aims and objectives, and make sure it has controls and mitigation measures in place to minimise those risks.

4.2 Not having risk management procedures in place could result in a failure to identify and monitor risks, or apply appropriate and proportionate mitigation measures. It is also important to bear in mind:

- Our stakeholders and public expectations that we manage risk effectively;
- The demands of legislation and external bodies, such as regulators and auditors;
- The value of risk management in making informed decisions about the effective use of capital and resources, and in reducing costly mistakes or firefighting;
- The desire to make the organisation a better and safer place to work, and for others to work with.

4.3 By practising risk management we will:

- Limit the impact of identified threats to the delivery of our objectives
- Acknowledge and manage opportunities which may be of benefit to the organisation
- Develop and promote positive risk management culture and behaviours
- Effectively manage and promote confidence in our internal risk management controls.

5. Roles and Responsibilities

5.1 Board

The Board have overall responsibility for risks taken by the organisation, and review the Corporate Risk Register once a year. The authority to manage and review risks is delegated to the Audit and Risk Committee.

5.2 Audit and Risk Committee (ARC)

The Audit and Risk Committee oversees the development and operation of risk management at a strategic level, and regularly reviews the Corporate Risk Register, as well as Project Risks which are deemed strategic. The Audit and Risk Committee are responsible for providing assurance to both the Board and Accountable Officer that risks within the organisation are appropriately managed.

5.3 Accountable Officer

The Accountable Officer is responsible for ensuring that there are sound and effective arrangements for internal control and risk management. They are advised by both the Board and Audit and Risk Committee, who have a key role to advise on risk tolerance, risk appetite and the management of risk within the organisation.

5.4 Executive Team

The Executive Team is responsible for monitoring and managing risk across the organisation and making sure we have effective policies and procedures in place. The Executive oversees the review of the Risk Management Policy and Corporate Risk Register, with support from the Corporate Performance Manager. Any significant corporate issues relating to risk management are brought to the Audit and Risk Committee's attention.

5.5 Operational Managers

Operational Managers are responsible for making sure risk management is embedded into their areas of responsibility, that risk owners and all other staff are aware of its importance, and that appropriate mitigation measures are in place.

5.6 Project Managers

Project Managers are responsible for the Project Risk Registers, which focus on project activities. They will review their risk registers on a regular basis (at least every six weeks, or when circumstances change significantly) and make sure their risk registers are updated accordingly. They will bring Project Board's attention to any concerns or instances where ineffective risk management is impacting on our business or the achievement of its key aims and objectives.

5.6 Risk Owners

Risk Owners are responsible for monitoring and managing their assigned risks on a day-to-day basis. They will review their risks on a regular basis (at least every six weeks, or when circumstances change significantly) and make sure their risk registers are updated accordingly. Risk Owners will bring their Project Managers' attention to any concerns or instances where ineffective risk management may be impacting on our business or the achievement of its key aims and objectives.

5.7 Other staff

Risk management is not a specialist activity or only for nominated "Risk Owners". It is a core part of everyone's job, and should be embedded throughout the organisation and its activities. A risk assessment should be part of planning and implementing all activities, with risks identified and mitigation measures put in place.

5.8 Training

Regardless of the role our staff take in managing risk within the organisation, as a minimum, all staff should complete the Risk Management Learning Module within ELMS.

6. Risk Registers

6.1 Types of register

We maintain a strategic Corporate Risk Register and a Projects Risk Register for Projects.

6.2 Corporate Risk Register

The Corporate Risk Register is a confidential document which sets out the "across the board" risks that could threaten our core business and the way it operates. The Corporate Risk Register is maintained on our R Drive. (insert link)

6.3 Project Risk Register

The Project Risk Register identifies risks that could threaten project activities. This register is maintained by the Project Team, and is reviewed by the Project Board. Where necessary, Project Board has the ability to escalate a risk to the Corporate Risk Register, if appropriate.

Any risks sitting above the agreed tolerance limit are escalated to the Audit and Risk Committee for noting and discussion if needed. The Project Risk Register is maintained our R Drive. (insert link)

6.4 Format

All registers have the following information:

- Area impacted by the risk (financial, legal/compliance/regulatory, operational, reputational, people/knowledge, environmental, political and public)
- Risk name and description
- Date entered on risk register
- Initial risk scores (likelihood and impact)
- Tasks to mitigate the risk (controls/safeguards/precautions)
- Revised risk scores (likelihood and impact)
- Additional actions required
- Risk owner (by job title)

7. Risk types

7.1 There are 4 types of risk which are widely recognised;

Internal	The organisation has some control over these risks. They can be managed using internal controls and mitigating actions involving risk registers, controls and assurances.	Examples of this type of risk include; • Health & Safety • Security • Infrastructure
External	The organisation must consider its resilience to major events taking place in the wider world. It can sometimes be difficult to assess the likelihood of these events, but it is possible to assess the impact that an external event would have on the organisation. Resilience frameworks for these types of risk are outlined in the organisations business	Examples of this type of risk include; • Economic Downturn • Terrorist Attacks • Extreme weather • Cyber Attacks • Global Pandemics

Strategic	These are risks to the organisations purpose and objectives. These types of risk will jeopardise the achievement of objectives within their set timeframe. For example, the objectives set within the 5 year plan.	Examples of this type of risk include;
		• Immediate impact events which stop the organisation operating
		• Slow burning risks that gradually grow to prevent delivery of objectives
		  ○ Staff turnover
		  ○ Leadership capability

Major Projects	Projects are central to the work of the National Park Authority. Risks to the delivery of top priority projects should be considered by the Audit and Risk Committee. They will be specific to each individual project.	Examples of this type of risk include; • Shifting requirements • Slippage in timeframes • Failure to deliver

8. Risk categories

8.1 Our Risk Registers break down risk into a further 8 categories. A single risk can have one or many potential impacts.

8.2 Risk categories are important when thinking about risk tolerance and appetite. For example, our appetite for environmental risk may differ from our appetite for financial risk.

Financial	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.
Legal / Compliance / Regulatory / Governance	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). This could also include risks arising from unclear plans, priorities, authorities and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance.
Operational	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. This could also include risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.
Reputational	Risks arising from adverse events, including ethical violations, decisions where sustainability has not been duly considered; where corporate decisions are at odds with organisational policy; systemic or repeated failures; poor quality or a lack of innovation, leading to damage to our reputation and/or destruction of trust and valuable relationships. This could also include risks arising from a failure to prevent unauthorised and/or inappropriate access to National Park Authority assets, systems and/or information held, including cyber security and non-compliance with GDPR requirements.
People / Knowledge	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.
Environmental	Risks arising from any source of harm, danger or damage to the environment, for example, from natural hazards, pollution or depletion of natural resources; this includes transmission in, or through, the air, water or soil. This could also include risks arising from climate change, biodiversity loss or negative ecological impact. Similarly, this includes risks that arise from negative environmental and climatic impacts, such as extreme weather and storm events leading to flooding and landslides, and changes to environmental conditions such as algal blooms or droughts that have the ability to impact our assets and operational activities.

Political	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).
Public	Risks arising from adverse events that may have an impact on the quality of life of the general public, for example, path closures to enable maintenance and/or disruption of service, such as at the Slipway.

9. Risk Appetite and Tolerance

9.1 The organisations Risk Appetite reflects the amount and type of risk that we are willing to take. Risk Tolerance reflects the organisations readiness to bear that risk in order to achieve its business objectives. Simply put how much risk are we willing to take to achieve our goals, and are we suitably prepared to take it.

9.2 *"The Orange Book – Management of Risk, Principles and Concepts"* (2019), and subsequent UK Government publications provide the following definitions;

- **Risk Appetite**: the level of risk with which an organisation **aims** to operate.
- **Risk Tolerance**: the level of risk with which an organisation is **willing** to operate.

9.3 We have a separate Risk Appetite Statement which should be read in conjunction with this policy and can be found here (INSERT LINK). This statement is reviewed at least every 6 months by the Audit and Risk Committee, and once a year by the Board.

10. Assessing risk tolerance levels

10.1 We assesses risk against the matrix and scoring descriptions in Tables 1 to 4. For each risk, the dimension scores of **likelihood** and **impact** are multiplied to produce an **initial risk score**. When mitigation measures are identified, the two dimensions are scored and multiplied again to produce a **revised risk score**. This score is categorised as being an acceptable, adequate, tolerable and unacceptable **level of tolerance**. Where a risk covers more than one of the Impact categories, then the highest likelihood and impact score should be selected.

Table 1 – Risk scores matrix

Likelihood						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Impact				

Table 2 – Likelihood definitions

Definition	Rating
The event is expected to occur	5
The event will probably occur	4
The event may occur at some time	3
The event is not expected to occur in normal circumstances	2

The event may occur only in exceptional circumstances	1

Risk Management Framework - DRAFT

Table 3 – Impact definitions

	1	2	3	4	5
Descriptor	**Negligible**	**Low**	**Moderate**	**Significant**	**Severe**
Operational	Some service/delivery interruption but can be made up without external parties becoming aware. Complaint possible but unlikely. FOI/EIR possible but unlikely. Petition unlikely.	Small fall in service/delivery levels, some minor quality standards are not met. External parties unlikely to become aware. Complaint possible. FOI/EIR possible. Petition possible.	Moderate fall in service/delivery levels. External parties aware and relationships strained. Projects likely to be delayed. Complaint expected. FOI/EIR expected. Petition expected.	Significant fall in service/delivery levels, project deadlines not achieved, AOP/5 Year Plan/NPPPP targets adversely impacted. Small number of complaints expected (<20). Petition of less than 10,000 signatures.	Serious fall in service/delivery levels, likely to result in increased scrutiny from SG/external funders. Large number of complaints expected (21+). Petition of more than 10,000 signatures.
Reputational	Public concern unlikely to have any lasting effect. No measures required to correct the situation. Complaint possible but unlikely.	Minor adverse public or media attention or complaints. No special measures needed beyond normal operations. Complaint possible.	Attention from the media or public in a local area, localised community/partner relations at risk but damage likely confined to one local authority area. Complaint probable (<10).	Attention from the media or public across two or more local authority areas, or nationally. Media/stakeholder relations handling required to respond to situation – comms/stakeholder engagement plan required. Stakeholder relations at risk and damage unlikely to be contained. Small number of complaints expected (<20).	Significant and sustained adverse national media coverage. Proactive Communications Plan required including ongoing media handling. Large number of complaints expected (21+)
People / Knowledge	Short term low staffing level temporarily reduced service quality.	Ongoing low staffing levels reduces service quality. Risk of minor injury to people increased as a result of action/inaction.	Late delivery of key objective/service due to lack of staff. Ongoing unsafe staff level. Serious injury to at least one person as a result of action/inaction.	Uncertain delivery of key objective/service due to lack of staff. Critical unsafe staff level. Serious injury to a large number of people as a result of action/inaction.	Non-delivery of key objective/service due to lack of staff, loss of key staff, unable to deliver service due to staff levels. Fatality as a result of action/inaction.
Financial	Negligible impact on either SG or external/commercial funding. Strong relationships with funder, with regular communication and updates provided. No risk to funding. Financial impact (positive or negative) of up to £25k	Low impact on either SG or external/commercial funding. Relationships with funder are good and communications are maintained. No risk to future funding. Financial impact (positive or negative) of up to £50k	Moderate impact on either SG or external/commercial funding. Management required to ensure the relationships are maintained. Low risk to future funding, Financial impact (positive or negative) of up to £100k	Significant impact on either SG or external/commercial funding. Breakdown of relationship is significant but repairable - further funding in the future could be at risk. Financial impact (positive or negative) of up to £200k	Serious impact on either SG funding or external/commercial funding. Irreparable breakdown in relationship resulting in low chance of future funding. Financial impact (positive or negative) of over £300k
Political	Little political impact or consideration required. Will not involve a change of policy and further funding considerations. May receive a small (<2) number of enquiries from MSPs/local Councillors.	Little political impact or considerations required. Will not involve a change of policy and further funding considerations. May receive a small (<7) number of enquiries from MSPs/local Councillors.	Some political impact or considerations required. May involve a change of policy and further funding considerations. Will receive a moderate number of enquiries from MSPs/local Councillors (<15).	Will have political implications that we are able to influence, but could affect our 'licence to operate'. Will involve a change of policy and may involve future funding considerations. Will receive a large number of enquiries from MSPs/local Councillors (15-30)	Will have far reaching political implications that are outside our control and will undermine our 'licence to operate'. Significant involvement and input from SG required. Will involve a change of policy and further funding considerations. Will receive a significant number of enquiries from MSPs/local Councillors (30+)
Legal / Compliance / Regulatory / Governance	Regulatory, statutory compliance or other legal obligation. Litigation very unlikely.	Regulatory, statutory compliance or other legal obligation breach with will require to be reported to the regulator including routine notification; no penalties likely. Litigation unlikely.	Regulatory, statutory compliance or other legal obligation breach which will require to be reported to the regulator; minor penalties (monetary and non-monetary); closure of some facilities in short-term until compliance met Litigation probable.	Legal obligation breach; with penalties (monetary and non-monetary including public reprimand); closure of facilities, sites and other buildings for medium-term until compliance met Litigation probable.	Significant penalties (monetary and non-monetary including public reprimand); closure of sites and buildings for long-term Major litigation expected.
Environmental	Insignificant impact on the environment.	Minor impact on the environment with no lasting effects.	Limited impact on the environment with short term or medium term effects (resolved within 1 to 5 years)	Significant impact on the environment with medium to long term effects (resolved 5 years +)	Serious long term impact on the environment and/or permanent change.
Public	Little or no impact on members of the public (e.g. short term (less than one month) temporary disruption to way of life) Complaint possible but unlikely. FOI/EIR possible but unlikely.	Small impact on members of the public (e.g. medium term (less than three months) temporary disruption to way of life, injury unlikely). Public may have a perceived loss. Complaint possible. FOI/EIR possible.	Medium impact on members of the public (e.g. long term (over six months) temporary disruption to way of life). Public will have a perceived loss Complaint expected. FOI/EIR expected.	Large impact on members of the public (e.g. temporary closure of a site for over a year). Public perception may be that we are not doing enough/doing things in the wrong way. Small number of complaints expected (>20).	Serious impact on member of the public (e.g. temporary closure of a site for up to two years, or permanent closure of a site). Public perception will be that we are not doing enough/doing things in the wrong way. Large number of complaints expected (21+).

Table 4 – Risk level tolerance

Total score	Risk treatment
17 – 25 Unacceptable	Risks are so significant that risk treatment is mandatory and all activity should stop until the risks are mitigated appropriately
10 – 16 Tolerable	Risks are so significant that risk treatment is mandatory within specified timescale
6 – 10 Adequate	Risks should be kept under regular review, with revision to risk mitigation and rating, where appropriate
1 – 4 Acceptable	Risks can be regarded as negligible, or so small that no risk treatment is required, however controls should be maintained

10.2 When a potential new action or objective is assessed for risk, either Project Board or Executive Team will review the revised risk score suggested by the risk owner to make sure it is robust and reasonable. This is kept under continuous review by both Project Managers and Project Board, where appropriate.

10.3 Where a risk score reaches the tolerance level of 17 or above (unacceptable risk) post-mitigation, the Chief Executive will immediately bring the risk to the attention of the Convener as well as to the Chair of the Audit and Risk Committee.

11. Risk Escalation

11.1 There are a number of trigger points within our risk registers that escalate a risk to the next level for monitoring. These are set out below for both Corporate Risks and Project Risks.

Project risks will only routinely be escalated to Audit and Risk Committee where they contain strategic risks; Audit and Risk Committee have the authority to request sight of Project Risk Registers should they wish.

11.2 Individual Project Risk Registers

Trigger Point (post mitigation)	**Action**
10 to 16	When a risk on an individual Project Risk Register is scored between 10 and 16 inclusive, this should be escalated to the next Project Board meeting, with a clear outline of risk mitigations in place, and a date the risk is expected to be closed.
17 to 25	When a risk on an individual Project Risk Register is scored at 17 or above, this should be escalated to Project Board immediately, with a clear outline of risk mitigations in place, and a date the risk is expected to be closed. Project Board will review the mitigations proposed, add any further mitigations required and will ensure monitoring of the risk via regular Project Board meetings.

11.3 Projects Risk Register

Trigger Point (post mitigation)	**Action**
17 and above	When a risk on the Project Risk Register is scored at 17 and above, Project Board will take a considered view as to whether this should be escalated to the Corporate Risk Register.

	This view should consider the date the risk is expected to be closed, the overall project status, whether any further mitigations are likely to reduce the risk, whether the risk has a strategic impact and whether there is public / board interest in the progress of a particular project.

11.4 Corporate Risk Register

Trigger Point (post mitigation)	**Action**
10 to 16	When a risk on the Corporate Risk Register is scored between 10 and 16 inclusive, the Executive Team will consider whether this requires the immediate attention of Audit and Risk Committee. This view should consider the date the risk is expected to be closed, the overall project status, whether any further mitigations are likely to reduce the risk and whether there is public / board interest in the progress of a particular project.
17 to 25	When a risk on the Corporate Risk Register is scored at 17 or above, this should be escalated immediately to the Convenor of the Board, and the Chair of Audit and Risk Committee. The Convenor and Chair will review the mitigations proposed, add any further mitigations required and will ensure monitoring of the risk via Audit and Risk Committee.

12. Risk management tools

12.1 Risk identification

Identifying a new risk can happen any time, but is most likely:

- When we take on a new responsibility, scheme or project;
- As a result of an unforeseen incident or event; or
- As part of the regular review of risks by Executive or Directorate teams.

12.2 Risk statements

A marker of a good quality risk statement is that it can answer the following questions:

- What could happen?
- Why could it happen?
- Why do we care?

The key to writing a good risk statement is having a foundational understanding of risk components and their interrelationships. Understanding key risk-related terms and their definitions, as well as the business and its objectives, will result in more impactful risk articulation.

Within our organisation, we write risk statements using the following structure: [Event that has an effector on objectives] **caused by** [cause/s] **resulting in** [consequence/s]

Example*: Inability to carry out site risk assessments* ***caused by*** *lack of availability of appropriately qualified staff* ***resulting in*** *a delay in project timeline by 1 week and potential requirement to repay small amount of funding.*

Example: *Personal data breach* ***caused by*** *use of inappropriate data collection method and lack of staff training* ***resulting in*** *a fine of up to 4% of annual turnover.*

Example: *High employee turnover* ***caused by*** *job dissatisfaction and/or uncompetitive remuneration* ***resulting in*** *loss of corporate knowledge and delay in delivery of business objectives.*

12.3 Risk mitigation
Once a risk is identified, mitigation measures need to be considered. Initially, this can be defined simply as "tolerate, transfer, treat or terminate".

12.4 A new risk should be reported to the appropriate person as soon as possible by any officer so it can be entered in the relevant Risk Register. The Executive/Projects Team will then assess whether the risk should be entered in the Corporate Risk Register or escalated to Audit and Risk Committee.

12.5 When a new corporate risk is identified, Executive Team will assess the mitigating measures in place or proposed, and whether these will manage the risk to "as low as reasonably practicable". This process looks at whether the likelihood and impact of the risk is addressed adequately, and whether we need to enter into the risk, assuming it is optional, bearing in mind how the activity itself will further our objectives and the level of risk associated with it.

13. Equality and Diversity Impact Assessment (EqIA)

13.1 An equality and diversity impact assessment was carried out and no discriminatory effects were identified for any particular group within the workforce. This will be monitored on an ongoing basis. We are committed to making our services easy to use for all members of the community. In line with our statutory equalities duties, we will always ensure that reasonable adjustments are made to help customers access and use our services. If you want this information in another language or format, such as large font, please ask us and we will do our best to help meet your requirements.

14. Best Value

14.1 The policy meets the best value criteria, specifically in terms of governance and accountability, as a public authority our working practices are subject to public scrutiny and our decision making cannot be called into question. In addition, effective identification and management of risk is required across all of our business activities to ensure that we have considered risks appropriately.

15. Review timetable

15.1 In addition to the regular reviews by risk owners, all Risk Registers should be reviewed regularly to consider whether:

- The identified risks are appropriate and up-to-date
- The actions and controls in place are adequate and appropriate
- The revised risk score is appropriate
- Any additional action is needed to help mitigate the risk
- Any new risks should be added to the Register, either for new activities or for existing activities where the risk level may have increase.

The review timetable for each Risk Register is set out below:

Risk Register	Review Frequency	By Whom
Individual Project Risk Register	At least every month	Project Team
Project Risk Register	At least every six weeks	Project Board

Corporate Risk Register	At least every three months	Executive Team

15.2 The Corporate Risk Register will be reviewed by the Audit and Risk Committee at least twice a year. Where a risk score has increased, the reasons for the change will be set out.

15.3 The Corporate Risk Register will also be reviewed the by Board once a year.

Risk Management Framework - DRAFT

Risk Appetite Statement Appendix A

1. Introduction

This appendix provides information on the organisation's appetite to risk. It sets out our approach to risk as well as a framework for the level of risk appetite which can be pursued to achieve our objectives. It also provides details on how our risk appetite should be employed to help inform decision making, particularly at the strategic level.

2. Areas of risk

2.1 As a non-departmental public body responsible for Loch Lomond and the Trossachs National Park, the areas of risk we may be exposed to relate to the following categories:

- **Financial** – the decisions and risks we take in relation to the spending of the organisation.
- **Legal/Compliance/Regulatory** – our compliance will all relevant laws, regulations and governance requirements in the delivery of our duties.
- **Operational** – the decisions we take to how we operate and structure the organisation, including our internal business process and delivery model, and the use of supporting equipment.
- **Reputation** – the decisions, actions, response or position we take in relation to the scope of our work.
- **People/Knowledge** – the decisions we take in how we will deploy and utilise our resources to maximise their public value.
- **Environmental** – the policies, decisions, advice and choices we make about the management of nature, or from other's policies or from natural, political and socio-economic events.
- **Political** – the political impact of the policies, decisions and choices we make to further our objectives.
- **Public** – the public impact and perception of the policies, decisions and choices we make to further our objectives.

3. Risk Appetite

3.1 Our risk appetite is a statement of the level of risk it is willing to accept across the range of its activities. It enables the organisation to better communicate around issues of risk and assists members and Executive Team in their decision making roles, both formally and informally. When reviewing risk registers, managers will be able to better assess if additional mitigations or actions are required to address risks.

3.2 The overall appetite to risk is currently assessed as "**Cautious**" i.e. that the organisation is willing to consider making decisions to deliver our Corporate Plan which may involve a small degree of risk taking in order to achieve the desired benefits. This would only be undertaken however where the relevant risks are judged to be within the organisation's capacity to manage them.

3.3 Each category of risk has been assessed by Operational Managers and the Executive Team, prior to review by the Board as to the appropriate risk appetite level. This provides a framework to help inform decision making. This looks at the level of risk which is deemed to be "manageable" i.e. where the risks will need careful management but are considered to be worth taking. Where potential risks could breach the "manageable" level, assurance should be provided to the Board and Executive Team that these can be appropriately controlled.

4. Risk Appetite Evaluation Map

4.1 The following chart displays the organisation's risk appetite using a Risk Appetite Evaluation Map. The coloured bar represents the level of risk which the organisation regards as the 'manageable' zone. This reflects that any risks that fall within this zone will need careful management but are considered to be worth taking. Any potential risks above the bar are in the 'dangerous' zone and represents risks which the organisation is unlikely to take. Risks below the bar are viewed as being in the 'comfortable' zone where the level of risk does not pose a major threat as long as it is managed sensibly.

Risk Appetite Levels	Averse	Minimal	Cautious	Open	Hungry
Financial	← COMFORTABLE →	MANAGEABLE	←	DANGEROUS →	
Legal/Compliance/ Regulatory/Governance	COMFORTABLE	MANAGEABLE	←	DANGEROUS →	
Operational	← COMFORTABLE →		MANAGEABLE	← DANGEROUS →	
Reputational	← COMFORTABLE →		MANAGEABLE	← DANGEROUS →	
People/Knowledge	← COMFORTABLE →	MANAGEABLE	←	DANGEROUS →	
Environmental/Nature	COMFORTABLE	MANAGEABLE	←	DANGEROUS →	
Political	COMFORTABLE	MANAGEABLE	←	DANGEROUS →	
Public	← COMFORTABLE →		MANAGEABLE	← DANGEROUS →	
	(Very Low)	(Low)	(Medium)	(High)	(Very High)

4. 2 Definition of each level of risk appetite are:

- **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
- **Minimal** – 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 my 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.
- **Hungry** - 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.

5. Employment of Risk Appetite

5.1 The Risk Appetite Evaluation Map provides a framework to help inform decision making and along with the supporting narratives shapes our approach to risk taking. As such, decisions which require approval by the Executive Team or Board should ensure that the potential risks are within the organisation's risk appetite. It is acknowledged however that decisions will be taken on a case-by-case basis and where any risks are assessed to fall out with the "manageable zone" then the author and sponsor should provide assurance to the Executive Team/Board that the risks are considered to be worth taking and can be suitably managed.

5.2 To assess whether the relevant risks are within the organisation's risk appetite, staff should utilise the generic scoring guidance (see page 5 and 6 of Risk Management Policy). This provides a numerical score on the likelihood and impact of the risk. When combined, this provides a risk rating which can be mapped against the "Risks Appetite Evaluation Map" using the appropriate category of risk (see Risk Appetite Evaluation Map above). In general, those risks which are assessed at the lower end of a "high" rated risk are likely to be within the "manageable" zone. Where strategic decisions are likely to involve multiple risks, then the assessor should make an overall assessment.

5.3 Authors and sponsors of Executive Team and Board Papers should ensure that they comment on any risks regarding their proposals and confirm that they align to the organisation's risk appetite.

Risk Management Framework - DRAFT

Document Control Sheet Appendix B

Prepared By	Corporate Performance Manager
Date Effective From	
Review Frequency	Reviewed regularly and updated as required in relation to changing situations and lessons learned.
Contact	Corporate Performance Manager

Revision History:

Version:	Date:	Summary of Changes:	Name:
0_1		New procedure	

Approvals: This document requires the following signed approvals.

Name/Title	Date	Version
Executive Team		

Distribution: This document has been distributed to

Name:	Title/Division:	Date of Issue:	Version:
All Staff			