YORKSHIRE DALES
National Park Authority

Risk Management Policy

(approved A&R Committee, 12 November 2013; Review Date November 2018; interim review undertaken by SMT 26 July 2017: changes made to requirements to maintain service-specific risk registers, at paragraphs 35 and 36)

1. The Yorkshire Dales National Park Authority is committed to an effective process of business risk management, and has a requirement to maintain and keep under review adequate arrangements for managing those risks which threaten the Authority's ability to deliver services in the most efficient, effective and economic way, and to achieve value for money. The Authority therefore needs to ensure that a process exists for identifying, analysing and managing any risk or threat to the organisation or its resources, including ensuring that those resources are protected from the risk of loss, damage or misuse.

2. The purpose of risk management is to increase the likelihood that the Authority will achieve its key objectives, as set out in the Corporate Plan, whilst avoiding financial loss, damage to service reputation, or prejudice to continued effective service provision. This involves systematically:

- identifying risks;
- evaluating exposure to the risks identified;
- assessing the control measures in place to deal with the risks; and
- managing those risks in a planned way.

3. Risk management has the following aims:

- Protect service delivery and its quality
- Protect the reputation and image of the organisation
- Ensure the security of the organisation
- Secure earning capacity and funding
- Secure the wellbeing of employees and service users
- Ensure the integrity and resilience of information systems
- Ensure probity and ethical conduct
- Avoid criminal prosecution and civil litigation
- Avoid financial loss, fraud or corruption
- Inform and enhance performance management.

4. Ultimately, risk management is the responsibility of the Chief Executive and of the whole Membership of the Authority, who together have a responsibility to maintain a sound system of internal control that supports the achievement of the Authority's policies, aims and objectives, and to exercise strong stewardship to safeguard public funds and assets. Each year the Chief Executive and the Chairman are required to make an **Annual Governance Statement**, which forms part of the public reporting process alongside the annual accounts. The Audit & Review Committee also has an important role to play in risk management, as set out in paragraph 11.

RISK MANAGEMENT PRINCIPLES

5. This policy outlines the key aspects of the risk management process, which are:

- Roles and responsibilities;
- Organisational structure;
- Risk identification and evaluation;
- Recording and monitoring;
- Awareness and training; and
- Evaluation of the effectiveness of risk management arrangements.

6. Risk management must operate throughout the organisation, and be embedded in processes such as business planning, target setting, performance management and staff appraisal. The extent to which this is achieved will be monitored under the evaluation arrangements described in this policy.

7. All reports to the Authority or its committees will include a section which summarises the main risks associated with the subject matter of the report, **but only wherever a material risk is associated with the content of that report**.

8. The objective of risk management is not to totally eliminate risk, but to reduce it to an acceptable and cost effective level. The approach to managing any particular risk may be (or include elements of) acceptance, reduction, elimination or transfer of the risk. This is arrived at by the application of the manager's knowledge and expertise, and by determining the level of risk which is acceptable in meeting the organisation's business objectives. The Chief Executive and Members should be comfortable that their assessment of the acceptance of residual risk aligns with the manager's evaluation.

9. Whilst managers evaluate controls through a process of self-assessment, the organisation also has a number of assurance activities and providers, which give independent assurance upon the effectiveness and on-going evaluation of the internal control environment, including:

- External Audit (provided by Deloitte LLP);
- Internal Audit (provided under contract by Veritau Ltd);
- the Audit & Review Committee.
- Inspections relating to various health and safety matters, including fire safety and Portable Appliance Testing (PAT)
- Investors in People and Customer Service Excellence accreditations

ROLES AND RESPONSIBILITIES

10. Overall responsibility for risk management rests with the Authority and with the Chief Executive.

11. The Authority has delegated to its Audit & Review Committee specific roles in relation to the monitoring and review of the effectiveness of the system of internal controls. In particular, the Audit & Review Committee has been designated as a forum to review the adequacy of the arrangements for corporate governance and risk management. The Audit & Review Committee also considers the annual internal and external audit plans (and any audit reports deriving from these), and seeks to ensure that they constitute an adequate programme, which addresses most of the main risks facing the organisation.

12. At Senior Officer level, the Monitoring Officer is designated as the officer who will lead on issues of corporate governance, and the Director of Corporate Services on risk management, both posts providing advice arising from actions to minimise risks. They will work closely together to achieve co-ordination of these key corporate processes.

13. The Senior Management Team (SMT) is responsible for implementing this policy, and in particular for:

- Compiling and maintaining the Authority's Operational Risk Register;
- Identifying and evaluating new risks;
- Encouraging good practice and a culture of risk management throughout the organisation.

14. Line Managers also have a vital role to play, both in identifying and managing risks within their sphere of responsibility, and in contributing to the process of risk management for the organisation as a whole.

15. Finally, front line services staff need to be aware of the risk management approach and processes at an operational level, so that they can contribute their own ideas and experience to the process of identifying and managing risk.

RISK REGISTERS AND THE RISK MANAGEMENT PROCESS

16. Risk registers provide a structured approach to:

- Identifying the risks that may stop the Authority from achieving its objectives;
- Assessing the probability and impact of those risks;
- Agreeing preventative or remedial actions to ensure that such risks are reduced to an acceptable level.

17. Risk registers help managers and other officers to understand the concepts around risk management and to see the links to service delivery, and to individual performance management objectives. They also provide a focus for managers to discuss their concerns in delivering service objectives and how specific risks can be overcome.

18. The Authority's Risk Management process is structured hierarchically and in a way that demonstrates:

- to our 'Corporate Plan' audience that we are aware of, and have plans to manage, the risks that could otherwise undermine the delivery of our corporate priorities (an **Annual Risk Management Plan**);

- to Audit & Review Committee members that we have an active process of identifying and managing 'higher level' or strategic risks (a **Strategic Risk Register**).

- to other 'specialist' audiences (e.g. our insurance brokers, concerning insurable risks; UNISON, concerning health and safety risks that might affect their members), that we have a detailed but appropriate approach to all the various components of risk (an **Operational Risk Register**; this to hold much of the specific detail about controls).

- to our auditors (and other external audiences), that we have a comprehensive approach.

19. Front line staff use their experience and ideas to inform line managers about risks which they encounter in their day to day work. Line managers use this information and their other experience to independently maintain a simple assessment checklist of the risks for their areas of responsibility, which they review in supervision meetings with their managers. Senior managers assess this information, and advise SMT whether changes are needed to the Authority's risk registers and risk management plans. Developing issues in terms of the main risks facing the organisation, the changing risk profile, and the steps taken to manage risks are communicated to the Audit & Review Committee.

20. The Authority determines the Corporate Plan, in the preparation of which the main risks facing the Authority will be considered, and from which can be derived the business objectives which form the starting point for risk analysis and management. The Authority may also issue instructions to the Audit & Review Committee about matters related to internal control and risk management which it wishes the Committee to examine. The Audit & Review Committee gives advice to SMT in relation to the issues referred to it, and in the light of the Authority's views. The decisions of SMT in relation to the strategic risk register are fed back by senior managers to line managers; and both at this level and between line managers and front line staff, appraisal targets will reflect decisions about the control of risks.

21. This information and decision flow process encompasses the role of the Chief Executive (who is an adviser to the Authority and to the Audit & Review Committee, and who 'line manages' SMT). The key outputs from the process are as described in paragraph 18, and which in turn feed into the Annual Governance Statement.

RISK IDENTIFICATION AND EVALUATION

22. The process for identifying risks has been described in the preceding section. All identified risks are scored against the likelihood of their materialising and for their impact if they did materialise. The next three tables describe this scoring system: **Table 1** identifies the 'likelihood' criteria, **Table 2** the 'impact' characteristics, and **Table 3** combines these two factors to give an overall classification ranging from 'Very Severe' to 'Manageable'.

Table 1

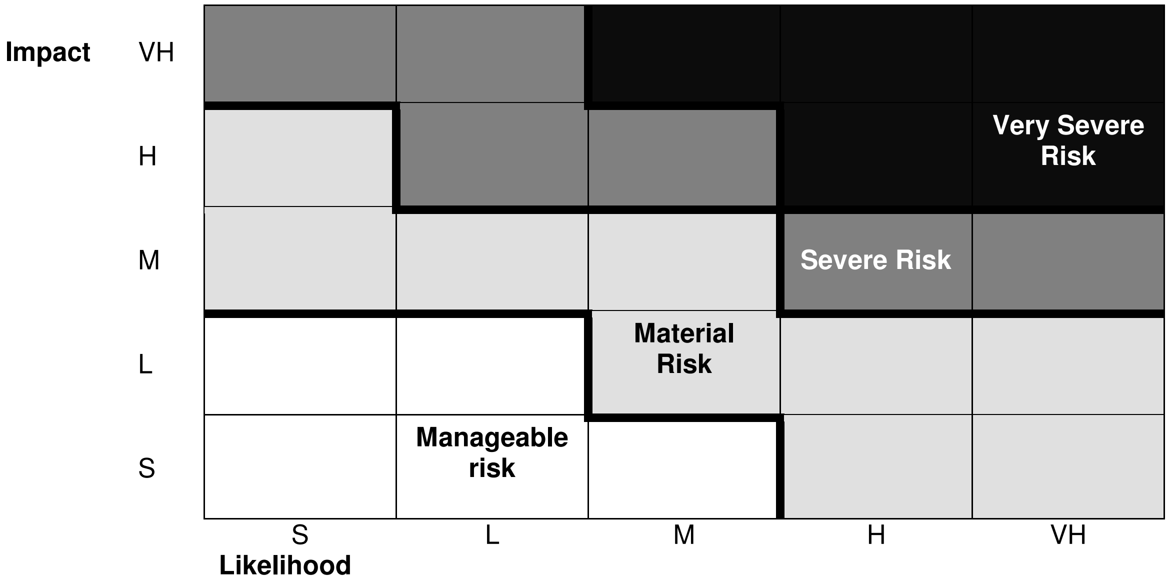
Risk **Likelihood** Ratings	
Probability	***Criteria***
Small	0-5% (extremely unlikely to occur)
Low	6-20% (unlikely but not impossible to occur)
Medium	21-50% (fairly likely to occur)
High	51-80% (more likely to occur than not)
Very High	>80% (almost certain to occur)

Table 2

Risk **Impact** Ratings	
Probability	***Characteristics***
Small	Minimal loss, delay, inconvenience or interruption. Easily and quickly resolved
Low	Minor loss, delay, inconvenience or interruption. Short to medium term effect
Medium	Significant waste of time and resources. Impact on operational efficiency, output and quality. Medium term effect which may be expensive to recover
High	Major impact on costs and objectives. Serious impact on output and/or quality and reputation. Medium to long-term effect and expensive to recover.
Very High	Critical impact on the achievement of objectives and overall performance. Huge

	impact on costs and/or reputation. Very difficult and possibly long-term to recover

Table 3



23. Table 3 identifies four classes of risk:

- **Very Severe** Risks are those which cause most concern: their materialisation would have a potentially disastrous impact on the Authority's reputation or business continuity; immediate and comprehensive action would be required.
- **Severe** Risks are also of significant concern, and should be covered by contingency plans: their materialisation would be severe but not disastrous, and some immediate action would be required, along with the development of an appropriate action plan.
- **Material** Risks have consequences that are not severe and which can be managed by contingency plans and more detailed action plans which can be developed later. But such risks still need regular monitoring.
- **Manageable** Risks are those that are inherent in most activities; the consequences of their materialising are generally not important enough to affect the whole business, and they can be managed during delivery. The status of such risks will be reviewed periodically.

24. Agreeing the scoring of particular risks is the responsibility of SMT, subject to any advice from the Audit & Review Committee. In determining the likelihood of a risk occurring, all factors, including existing control mechanisms, will be taken into account.

RECORDING AND MONITORING

25. The Strategic and Operational Risk Registers (paragraph 18) will be maintained by the Director of Corporate Services. These registers will record the assessment made from time to time by SMT of what risks exist that need to be recorded in this way; for each risk,

information will be included as to its significance and what existing controls are in place. The Annual Risk Management Plan (paragraph 18) will be prepared each year by SMT.

26. Where it is identified that the processes in place are insufficient to manage a particular risk to an acceptable level, then an action plan for addressing the risk will be prepared. This will identify: which senior manager is responsible for this action; a date for completion of the action; and a date for review of the risk.

27. SMT will formally review risk management at least annually and also whenever events require. Such events will include any major issues that have arisen since the last review, including any relevant findings from performance improvement or major project reviews. SMT will consider whether any risks should be added to, or removed from, the risk register, or whether their classification, in relation to impact and/or likelihood, should be changed. The Operational Risk Register will be maintained as a 'live' document and will be updated by SMT members as appropriate.

28. The Audit & Review Committee will receive an annual report on Risk Management (see paragraph 30). The Committee may decide that a special report or particular recommendations of the Committee require the Authority's attention at any time.

AWARENESS AND TRAINING

29. This policy is accessible to all Authority Members and to all employees of the Authority. The Authority is committed to a process of raising awareness in this area, and requires SMT to ensure that all officers have an appropriate understanding of this policy.

EVALUATION OF EFFECTIVENESS

30. The Audit & Review Committee will, on an annual basis (at their autumn meeting), evaluate the effectiveness of the arrangements for risk management. This evaluation will be based on a report to the Committee by the Director of Corporate Services, which will address the following issues:

- The latest Annual Governance Statement, and any issues arising from it;
- Whether Audit and Inspection reports received since the last annual evaluation highlight any particular strengths or weaknesses;
- Any major incidents which have occurred since the last evaluation;
- Any developments in good practice in this area; and
- The extent to which risk management is embedded in organisational processes.

This report will include copies of the Strategic Risk Register and the Annual Risk Management Plan.

SUMMARY OF RESPONSIBILITIES

31. **The Authority** will:

- Determine the annual Corporate Plan, taking account of the key risk issues facing the Authority's priorities;
- Receive an annual report in relation to the adequacy of risk management arrangements, forming part of the Annual Governance Statement;
- Consider appropriate risk assessments in relation to all items of business coming before it.

32. **The Audit & Review Committee** will

- Approve and keep up to date this risk management policy
- Understand the main risks facing the organisation, and satisfy itself that those risks are appropriately controlled
- Review the adequacy of arrangements for risk management within the organisation
- Consider the annual external and internal audit plans, seeking to ensure that there is an adequate programme which addresses those of the main risks facing the organisation which it is the Authority's power to control;
- Make periodic reports to the Authority, as and when appropriate, upon the status of the control environment

33. **The Chief Executive** will

- Publish annually an Annual Governance Statement, summarising the effectiveness of the Authority's internal controls, and state how this is underpinned through the process of identifying objectives and key risks
- Provide leadership in relation to the implementation of this policy
- Ensure that SMT takes responsibility for implementing this policy, and plays its role in relation to the compilation and maintenance of the Strategic Risk and Operational Risk Registers and of the Annual Risk Management Plan.

34. **The Director of Corporate Services** will

- Lead on the process of risk management within the organisation as a whole
- Maintain the Strategic and Operational Risk Registers for the organisation
- Report to the Audit & Review Committee upon the changing status of risks and the controls adopted, as appropriate
- Present an annual evaluation report to the Audit & Review Committee
- As directed by SMT, seek to raise awareness and provide training, in order to improve understanding of risk management within the organisation.

35. **All Senior Managers** will

- Take responsibility for managing specific risks – as allocated by the Strategic Risk Register – including developing and implementing action plans
- Collectively (as SMT) implement this policy, and take decisions on the identification and analysis of strategic and operational risks
- Encourage good practice and a culture of risk management at all levels of the organisation
- Set objectives and targets for their staff in the light of the main risks facing the organisation
- Perform a key link role between SMT and line management, to ensure that there is a two-way flow of information and experience
- Ensure that detailed operational risks are covered as a matter of routine by officers responsible for the areas of work such risks affect, including, where appropriate, through the maintenance of simple risk registers. This will be a routine process for 'corporate' functions (IT, Finance, Property, HR, Communications and Legal), as failures in these services have the potential to undermine the whole Authority.

36. **All Line Managers** will

- Where appropriate, maintain a simple risk register in relation to their areas of responsibility. This is a requirement for 'corporate functions (see above), but is unlikely to be required for other services, for which the risks will be captured by the Operational Risk Register. However, a separate risk register may be appropriate for some large and complex projects.

- Discuss the risks affecting a particular service with the officers concerned as a mater of routine management, and not least as part of the annual appraisal process, within which actions may be set that are intended to manage down any operational risk
- Feed ideas and information to their managers in relation to risk issues

37. **All frontline staff** will

- Identify risks to their everyday work, and report on these to their line manager
- Report to their line manager on the performance of objectives and targets set for them.