

**Committee:** AUDIT AND REVIEW

**Date:** 9 February 2007

**Report:** RISK MANAGEMENT POLICY

### **Purpose of report**

1. To inform Members about current strategic risks across the range of the Authority's operations, and to propose a revision of the Authority's Risk Management Policy.

### **Strategic Planning Framework**

2. The information and recommendation contained in this report are consistent with the Authority's statutory purposes and its approved strategic planning framework, and in particular its objective 'to manage all aspects of the Authority's business so as to make the most effective use of our resources' (Best Value Performance Plan 2006/07).

### **Background**

3. Past reports on Risk Management to this committee have provided a short summary of the risk management process, alongside a very extensive list of the risks the Authority is (or may be) facing, together with additional narrative of certain key or topical risks. The current Risk Management Policy, included within the Financial Regulations, is as follows:

"The Authority seeks to comply with risk management best practice, and to ensure that the components of risk within all of its operations are identified and evaluated. Those operations to which an unacceptable degree of risk attaches will not be pursued until such times as that risk can be managed within acceptable bounds: the Authority's policy is to manage risk, rather than to become risk averse, so ensuring that our business remains innovative but secure.

In the context of this policy, the following must be taken into account when implementing more formalised risk management systems:

- the need for pragmatism: the process is not intended to eliminate risk and not all identified risks can be addressed immediately. Furthermore, risks will still exist that have not been identified. What is important is a culture of continuous learning, with risk management processes being adapted according to lessons learned.
- avoiding overly complex processes: there is an important need to avoid risk overload. The risks that are identified should make common sense and should be linked to Members' top priorities and concerns. The focus should be on those risks that are significant in the context of the Authority's objectives and reputation.
- ensuring that the process to be followed fits in with local circumstances and culture. Officers need to decide on practices that are appropriate to their circumstances".

4. At the meeting of the Corporate Governance Working Group on 16 June 2006, this approach was discussed in detail, the outcome being a recommendation that the approach to reporting risk management be changed. Specifically, that:

- The categorisation of risks be reviewed, dividing Strategic Risks (which would warrant Member review) from Operational Risks (which are managed routinely by officers as part of their jobs, and which wouldn't form part of routine reporting).
- The risk management policy should be linked to the 'internal controls' review of the Authority that the Audit Commission undertake annually (and which relates to the Statement of Internal Control).
- The possibility should be considered of a more frequent (more than annual) review of strategic risks by the Audit & Review Committee.

5. These modifications have required a reworking of the Authority's Risk Management Policy, with the proposed revision included as **Appendix 1**. Although this is clearly a lot more extensive than the existing policy, it does not remove the need for pragmatism in establishing which risks are real and those which can and should be managed. Note that, in relation to the third bullet point (above), rather than more frequent reporting to the Audit & Review Committee, the policy proposes that the frequency of the Senior Management Team's review of strategic risks will be increased (see paragraphs 28 and 31 of Appendix 1). This reinforces the operational nature of risks, and avoids 'report overload', particularly when it is not anticipated that the strategic risks facing the Authority will change significantly within any particular year.

6. The proposed policy includes a Strategic Risks Register, which identifies the current major risks that the Authority needs to consider in its operation. These are the high-level risks, which have potential to affect the operation of the Authority as whole; **Appendix 1a** identifies 23 such key risks.

7. The various operations of the Authority also face a number of service-specific or operational risks. These had been included in previous versions of the Risk Register, but are deemed to be below the 'strategic' level defined above, and so have been removed. These risks are, however, not to be ignored and are managed as part of the responsibilities of a range of officers, and will form the basis of individual officers' risk assessments (see paragraph 18 of the proposed policy). For completeness within this report, these 'operational' risks are summarised within **Appendix 2**, although this list does not form part of the policy document; Members may wish to comment as to whether any of the risks on this list would be better classified as 'strategic'.

## **Conclusion**

8. The revised Risk Management Policy described in this paper represents an opportunity to clarify and consolidate the Authority's approach to this area, and to identify specific responsibilities for applying this policy.

## **RECOMMENDATION**

9. That Members agree:

- that the Strategic Risk Register contains all identifiable higher level risks which the Audit & Review Committee require to be monitored;
- to adopt the revised Risk Management Policy as presented.

**Richard Burnett**  
**Head of Finance & Resources**

24 January 2007

Background documents: none

## Risk Management Policy (proposed revision)

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 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 Best Value Performance Plan. This involves a process of 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. The implementation of an effective business risk management policy is designed to increase the probability of achieving the Authority's objectives, whilst avoiding financial loss, damage to service reputation, and prejudice to continued effective service provision.

4. Risk management therefore 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.

5. 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 a **Statement of Internal Control**, 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 below.

## RISK MANAGEMENT PRINCIPLES

6. 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.

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

8. 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.**

9. The objective of risk management is not to totally eliminate risk, but to reduce it to an acceptable, cost effective level. Any action plan for managing any particular risk may be (or include elements of) acceptance of the risk; reduction of the risk; elimination of the risk; or transfer of the risk. The aim is the most cost effective management of the risk. This is arrived at by the application of the manager's knowledge and expertise, and 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 acceptance of residual risk aligns with the manager's evaluation.

10. Whilst managers evaluate controls through a process of self-assessment, the organisation also has a number of assurance activities and providers, which help to provide independent assurance upon the effectiveness of internal control. Inputs from the following key assurance providers are used as evidence in an ongoing evaluation of the control environment:

- External Audit (provided by the Audit Commission or its appointees)
- Internal Audit (provided under contract by North Yorkshire County Council)
- The Audit & Review Committee

## **ROLES AND RESPONSIBILITIES**

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

12. 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 will seek to ensure that they constitute an adequate programme, which addresses most of the main risks facing the organisation.

13. At Senior Officer level, the Solicitor is designated as the officer who will lead on issues of corporate governance, and the Head of Finance & Resources on risk management, both posts providing advice and contingency planning arising from actions to minimise risks.

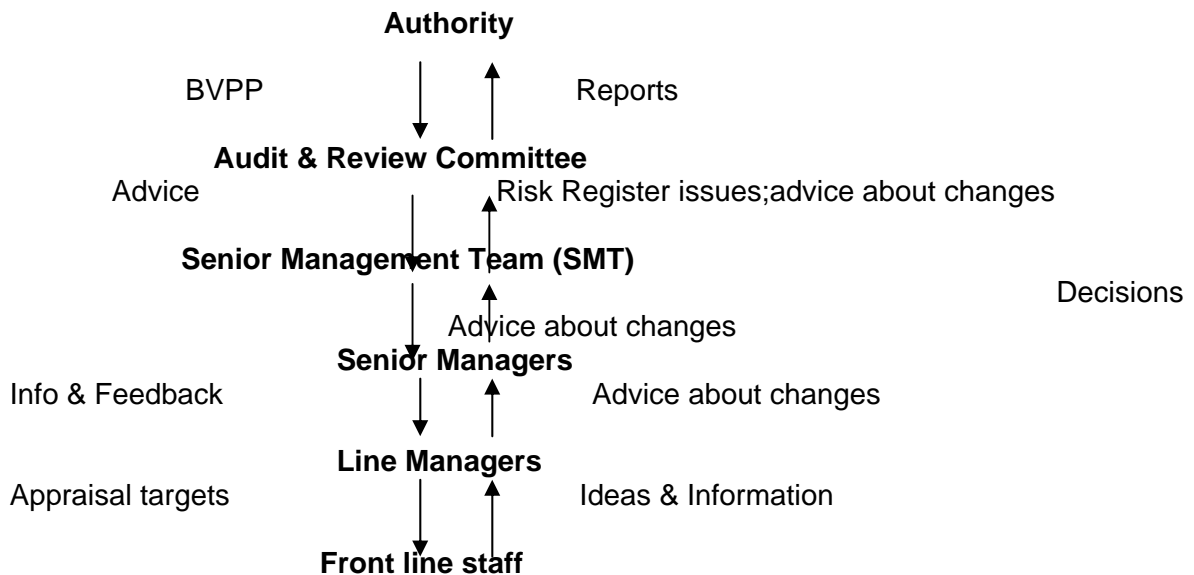
14. The Senior Management Team (SMT) is responsible for implementing this policy. It also plays a vital role in relation to the compilation and maintenance of the strategic risk register for the organisation. In this context, all members of senior management play an important role in relation to risk management, by encouraging good practice and a culture of risk management at all levels of the organisation; and by acting as key players in the identification and evaluation of risks, as explained in the next section.

15. 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, again as explained in the following section.

16. Finally, front line service staff need to be aware of the risk management approach and processes, so that they can contribute with their own ideas and experience to the process of identifying risks facing the organisation.

## ORGANISATIONAL STRUCTURE

17. The following diagram illustrates the flows of information and ideas within the organisation in relation to risk management.



18. The information flow that this diagram describes is as follows. Through the process of supervision, 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 operational risk register** for their areas of responsibility, which they review in supervision meetings with their managers (i.e. senior management). Senior managers assess this information, and advise SMT whether changes are needed to the **strategic** risk register for the organisation. 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.

19. On the other side of the process, the Authority determines the Best Value Performance 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 issues related to internal control and risk management (e.g. issues the Authority 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.

20. 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 the annual **Statement of Internal Control**; the identification

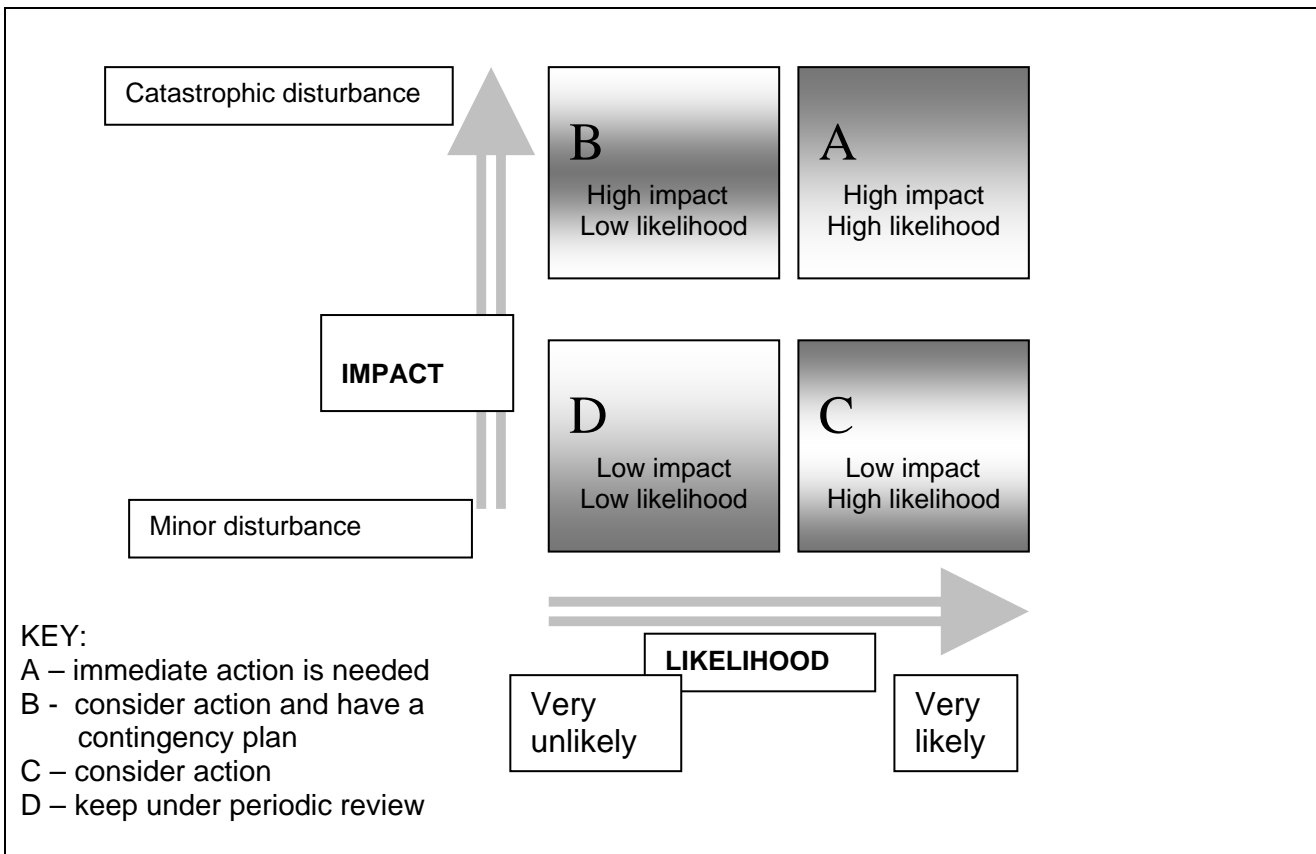
of key risks arising from the annual Best Value Performance Plan; the maintenance of an up to date risk register; and appraisal targets for staff.

21. All managers involved in this process, including the Chief Executive, will use supervision sessions with their staff to seek assurance that this policy is being implemented, insofar as it falls within the responsibilities of those staff.

**RISK IDENTIFICATION AND EVALUATION**

22. The process of how risks will be identified has been described in the preceding section. This process should also encompass identifying the existing control mechanisms, and developing ideas for an action plan.

23. All risks recorded on the register are scored for likelihood (low or high) and impact if they did materialise (low or high). Agreeing the value of these scores is the responsibility of SMT, subject to any advice from the Audit & Review Committee. Risks scored in this way will then be evaluated according to the following matrix:



24. In terms of impact:

- ‘Low’ means something which would be an inconvenience or irritant, but not a major problem
- ‘High’ means something which would cause major disruption, and would have a significant impact on service effectiveness

25. The above system will be used to determine which risks are the highest priorities for action. In determining the likelihood of a risk occurring, all factors, including existing control mechanisms, will be taken into account.

## **RECORDING AND MONITORING**

26. The Strategic Risk Register (**Appendix 1a**) will be maintained by the Head of Finance & Resources, and will record major 'headline' risks that may represent a threat to the operation of the Authority as whole. This register will record the assessment made from time to time by SMT of what risks exist that need to be recorded in this way, and, for each recorded risk, will include information on its impact and likelihood and what existing controls are in place.

27. 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.

28. SMT will consider the issue of risk management whenever events, and/or a change of circumstances, necessitate, and in any event not less than once a quarter (in February, May, August and November). This will involve considering any events which may have occurred since the last review, and also considering those risks on the Register where a review is warranted. In November and May of each year, SMT will also consider the strategic risk register overall, and in particular whether any risks should be added, removed, or their priority (i.e. impact and/or likelihood) re-evaluated.

29. The Audit & Review Committee will, from time to time, determine the frequency with which it wishes to monitor progress in relation to business risk management, and the Head of Finance & Resources will report to the Audit & Review Committee accordingly. The proceedings of the Audit & Review Committee are reported to the Authority as a matter of course, though the Committee may decide that a special report, or particular recommendations of the Committee, require the Authority's specific attention at any time.

## **AWARENESS AND TRAINING**

30. 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 adequate and appropriate awareness of this policy.

## **EVALUATION OF EFFECTIVENESS**

31. 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 Head of Finance & Resources, which will address the following issues:

- The latest Statement of Internal Control, and any issues arising from it;
- Audit and inspection reports received since the last annual evaluation, and whether they highlight any particular strengths or weaknesses;
- Any major incidents which have occurred in the period since the last evaluation;
- Any developments in good practice in this area; and
- The extent to which risk management is becoming embedded in organisational processes.

This report will include a copy of the Strategic Risk Register.

## **SUMMARY OF RESPONSIBILITIES**

32. **The Authority** will

- Determine the annual Best Value Performance Plan, in the light of the key risk issues facing the organisation

- Approve and keep up to date this risk management policy
- Receive an annual report in relation to the adequacy of risk management arrangements, within the annual Statement of Internal Control report.
- Consider appropriate risk assessments in relation to all items of business coming before it

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

- 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 most of the main risks facing the organisation
- Make periodic reports to the Authority, as and when appropriate, upon the status of the control environment

**34. The Chief Executive will**

- Publish annually a Statement of Internal Control, summarising the effectiveness of the organisation's internal controls, and state how this is underpinned through the process of identifying business 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 Register.

**35. The Head of Finance & Resources will**

- Lead on the process of risk management within the organisation as a whole
- Maintain the Strategic Risk Register for the organisation
- Report to the Audit & Review Committee upon the changing status of risks and the controls adopted
- 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

**36. 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 risks facing the organisation
- 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 (through the maintenance of simple risk registers: see below).

**37. All Line Managers will**

- Maintain a simple risk register in relation to their areas of responsibility
- Feed ideas and information to their managers in relation to risk issues
- Set objectives and targets for their staff in the light of the main risks within their area of responsibility

**38. All frontline staff will**

- Identify risks surrounding their everyday work, and report on these to their line manager

- Report to their line manager on performance of objectives and targets set for them.

## STRATEGIC RISK REGISTER

Category	Risk	Impact	Controls (Responsibility)
1. Reputation	1. <b>Contact with the public</b> (officers, members, volunteers).	A	Standing Orders; Declarations / registers of Interest (including Officers); employment clauses , inc. 'Non-political activity'; training and recruitment procedures; District Audit 'probity' reviews; (Members, Monitoring Officer); Member Code of Conduct and disciplinary procedure (Standards Board).
	2. <b>Poor Committee decisions.</b>	C	Standards Committee; Member training; Senior Officer – including Monitoring Officer - guidance; External Audit - Audit Commission - review & recommendations; officer professional training / competence.
	3. <b>Corruption, fraud and other illegal activities.</b>	B	Internal Audit; Treasurer role; Financial controls; Gifts & Hospitality Code of Conduct (Secretariat); Anti Fraud & Corruption procedure. 'Communications' network of contacts (whole Authority); prescription and separation of duties, including Scheme of Delegation.
2. Resources			
2.1 Financial	4. <b>Budget Failure</b> , including cash flow and working capital management.	B	Budgeting and monitoring process; professionally qualified staff; Financial Regulations; Treasurer; District Audit; DEFRA reporting (F&R Committee; Officers).
	5. <b>Funding risk:</b> failure to maximise grant income / over-reliance on primary funding; Earned income shortfalls.	B	Managed bid process with DEFRA; external funding group; partnership liaison (SMT); budgetary control and reporting (incl. to Senior Management and F&R Committee).
	6. <b>Inflation risk:</b> key when annual increase to settlement falls to below inflation (as is tied to wages increases).	C	Budget setting (especially long-term) and monitoring process.
	7. <b>Asset security;</b> theft and damage.	B	Financial Regulations & Accounting controls; asset registers; insurance; maintenance work (dedicated staff & budgets); car park cash collection contract; Alarm facilities & contracts. (SMT; Contracts Manager; Projects & Estates Officer).
	8. <b>Compliance with financial standards</b>	B	Professional officers, including Monitoring Officer & Solicitor, to identify and interpret new legislation; input from Members, District Audit, Treasurer (SMT).
	9. <b>Pension scheme</b> (risk of mismanagement and of runaway contribution costs).	B	Contracted in to NYCC scheme, with contribution rates set by third party actuarial valuation; regular reports to committee (Head of F&R). Risk assessment, and identification of counter measures, integral to annual Funding Strategy Statement.
	10. <b>Fraud, error</b>	B	Confidential Reporting policy; Internal Audit;

Category	Risk	Impact	Controls (Responsibility)
	(including expenses and collusive supplier fraud).		Treasurer role; Financial Regulations and accounting / financial controls; District Audit national fraud initiative; budgetary monitoring and managerial control.
2.2 Human Resources	11. <b>Recruitment</b> risks / difficulties.	B	Recruitment policies, including pre-employment health screening; psychometric testing. Monitoring market-rates of salary levels; Criminal Records Bureau appraisals where critical; employment references (Personnel & Training Officer). Training updates on recruitment to all staff involved in the recruitment process.
	12. <b>Loss of key staff.</b>	C	Retention clause in employment contracts for staff on pay bands B and above; developmental training, including management development, offered to staff to provide a degree of succession planning (SMT, P&T Officer). Use of secondments / 'acting up'; external contracting.
	13. <b>Failure to comply with legislation.</b> Liabilities arising from: Harassment, bullying, sexual assault, other violence, Discrimination, unfair dismissal; Failure to comply with employment legislation.	B	Professionally qualified Personnel staff; Monitoring Officer; advice from NYCC under Service Level Agreement; District Audit; guidance from central and local government; interaction with, and advice from, UNISON.
	14. <b>Hazardous working;</b> includes personal security / lone working.	B	Health & Safety procedures and policies, including appropriate training; compulsory risk assessment process; H&S working Group; insurance; reporting to SMT and F&R Committee.
2.3 Premises	15. <b>Physical damage:</b> Flooding and other extreme weather damage; Fire risk; Terrorism threat; other catastrophic event.	B	Emergency maintenance arrangements; Review of IT equipment proximal to flooding sources ; Insurance cover; IT back up and contingency plans; comprehensive fire safety process. (Senior Administration Officers).
	16. <b>'Health' of buildings:</b> Legionnaires Disease, vermin infestation, ventilation, asbestos.	B	Regular inspection of properties (Projects & Estates Officer; Head of External Affairs).
2.4 IT	17. <b>Network failure</b> across IT links.	B	Systems capable of independent operation; disaster recovery plan (Senior IT Officer),
	18. <b>Unauthorised access</b> and data security. Risk includes Viruses / hacking / sabotage.	B	Firewall and virus control software; password control; back-ups at main server sites; (SMT; Senior IT Officer).
3. Performance			
3.1 General	19. <b>'External'</b>	D	Civil Emergency Scheme; not primarily a risk for

Category	Risk	Impact	Controls (Responsibility)
	<b>catastrophes.</b>		the Authority, as NYCC / CCC have responsibility for managing the regional response to civil 'crises'.
	20. <b>Development control:</b> costs of major appeal / public inquiry / litigation.	B	(Head of Planning; Monitoring Officer).
	21. <b>Contracting:</b> procedural risk; poor tendering / contracting processes; financial stability of suppliers.	C	Financial Regulations (Contracts Officer; Monitoring Officer; Grant applicants in general).
3.3 Partnerships	22. <b>Failure to identify full joint liabilities.</b>	A	Management processes; insurance cover; Authority scrutiny (SMT).
3.4 Third Party liabilities	23. <b>Risks to public</b> whilst on our property or property we maintain; negligence / breach of statutory duty; corporate manslaughter.	B	Park Management and other maintenance work; third party liability insurance; risk assessments for planned work (Senior Admin. Officer, F&R; Contracts Manager, SMT); National Park Centres and Dales Countryside Museum (External Affairs)



## OPERATIONAL RISKS

Category	Risk	Priority
1. Reputation	1. Public relations & publicity (poor handling of complaints); press relationship; customer relations; defamation / libel risk.	B
	2. Proper standards of financial conduct; conflicts of interest; management integrity; sponsorship.	C
	3. Poor quality customer services.	B
	4. Authority processes damaging the environment.	B
2. Resources		
2.1 Financial		
	5. Going concern: identification of future financial costs.	B
	6. Leased vehicles: security, maintenance.	B
	7. General financial risk, including: Insurance; Petty Cash; failure to collect income due (e.g. grant funding); cash collection (DCM, events, car parking etc.); VAT; interest rates; exchange rates; payroll; Treasury Management; accounting system failure; debtors / creditors control (misstatement risk; over-provision; write-offs).	D
	8. Legality of financial transactions; proper accounting, including accurate and appropriate statutory financial reporting; adequacy of accounting for grants.	B
	9. Control over faulty goods / services received, incl. warranties.	D
	10. Retail (credit card sales; theft of inventory; stock write-offs; stock valuation).	C
	11. Excessive use of consumables (fuel oil, telephone, paper etc.).	D
2.2 Human Resources	12. Inadequate staffing levels / poor attendance (flexi-time, sick leave, excessive vacancies).	C
	13. Inadequate training & development; inflexible workforce; competence of members/staff / volunteers; Inadequate supervision of student placements.	B
	14. Insufficiently clear lines of authority /management.	B
	15. Non-compliance with H&S legislation.	B
	16. Poor performance where staff are unclear what their objectives are, or where there is poor co-ordination between departments, or low morale.	D
	17. Travelling dangers (to and at work): use of mobile phones; obstructions / hazards on road; adverse weather; Insurance checks relating to these issues.	B
2.3 Premises	18. General 'fit for purpose'; Disability Discrimination Act 1995.	D
	19. Maintenance (current status of building, identify requirements, manage maintenance to a controlled profile); car park surfaces & toilet maintenance.	C
	20. Utilities and systems: power cuts / surges; water supply; adequacy of external lighting / gritting policy; heating systems; safety of electrical and other mechanical equipment.	B
	21. Intruder and fire alarms.	B
	22. Access problems: damaged bridges, exits from premises onto highways.	D
2.4 IT	23. Legislation: Compliance with Data Protection Act 1998; Disability	C

Category	Risk	Priority
	Discrimination Act 1995.	
	24. E-mail & internet usage.	B
	25. Failure of key IT systems (accounts, GIS; PACS; telephony; e-retail).	B
	26. Insufficient or inadequate equipment.	C
	27. Offsite working (portables).	C
	28. Security and integrity: satellite sites; server rooms; use of unlicensed systems / software (includes general copyright infringements).	B
<b>3. Performance</b>		
<b>3.1 General</b>	29. Failure in management of the Authority; to plan strategically; inadequate policies and strategies.	B
	30. Failure to produce effective corporate plans or to create budgets for agreed business objectives.	B
	31. Failure to identify and evaluate project outcomes; unrealistic, non-strategic performance targets and Best Value indicators, leading to misdirected effort; use of poor management information.	B
	32. Involvement in projects which don't support primary purposes (or which contravene them).	C
	33. Resource & management problems caused by rapid growth / complexity of operations; errors / other staff failures due to increasing pressure / workload from new initiatives.	C
	34. Failure to provide statutorily-required services.	B
<b>3.2 Projects: other issues</b>	35. Inability to access sites (F&M; bad weather).	D
	36. Ongoing maintenance costs & risks associated with restorations (e.g. Craven Lime Works).	C
	37. Sub-contractor risk.	C
	38. Completion risk on construction projects.	B
<b>3.3 Partnerships</b>	39. Operational risks: Grant claims chain / confused accountabilities; hidden costs / extra bureaucracy / time wasting. Continuing costs where no exit strategy; loss of corporate identity / conflicts on ideology; pace of development: speed of slowest; loss of capability from sponsoring organisations (to the partnership); poor knowledge sharing and information flow.	B