Deloitte.

Cairngorms National Park Authority
Review of Risk Management
Internal Audit 2005/2006
August 2006
Strictly Private and Confidential

THIS IS A DRAFT REPORT AND REPRESENTS A WORK IN PROGRESS AND MAY CONTAIN PRELIMINARY RESULTS OR CONCLUSIONS INCOMPLETE INFORMATION OR INFORMATION WHICH IS SUBJECT TO CHANGE

Contents

Appendices

Deloitte.

Section 1 - Executive summary

1.1   Introduction

This review of Risk Management is part of our coverage of core operational areas as required in the audit plan approved by the Audit Committee. **Appendix B** shows the detailed scope and objectives of our review.

1.2   Background

The Cairngorms National Park Authority (CNPA) has developed its Risk Management Strategy and Risk Register following the Risk Management Workshop, facilitated by Deloitte in December 2004.

The Audit Committee approved the Risk Management Strategy and Risk Register in March 2005. CNPA reports to the Audit Committee on the progress of risk management on a quarterly basis. This is then reported to the Board on an annual basis as part of the annual report. All Board members receive Audit Committee papers to track progress throughout the year.

The Risk Management Strategy focuses on the Risk Register and states that all risks with an impact or likelihood scoring of 3.25 or more should be included in the risk register and should have associated action plans, responsible officers and timescales for completion attached.

The Risk Register records the top 22 risks to the organisation, all of which are ranked above 3.25 and each risk has an action plan in place, with a responsible officer and timescale for completion attached. All risks are linked to the Operational Plan, the key document from which the organisation operates.

The Management Team, comprising of the Heads of Group and Chief Executive within CNPA, review the Risk Register on a quarterly basis. These meetings are minuted by the Head of Corporate Services.

The Risk Register and Risk Management Strategy are held on a shared drive within the network, which all staff can access. However, as the risk management process is at an early stage of development, only the Management Team are routinely familiar with these documents at this time.

All expenditure of £5,000 within the organisation requires an Expenditure Justification Form to be completed. The form includes a Risk Assessment section. This form is presently being reviewed, with guidance notes being prepared for Project Officers.

Section 1 - Executive summary (continued)

1.2   Background (continued)

The Institute of Internal Auditors (IIA) has developed a Risk Maturity Cycle, which demonstrates the five key stages of risk maturity. These are:

- Risk Naïve – no formal approach developed for risk management;

- Risk Aware – scattered silo based approach to risk management;

- Risk Defined – strategy and policies in place and communicated. Risk appetite defined;

- Risk Managed – enterprise approach to risk management developed and communicated;

- Risk Enabled – risk management and internal controls fully embedded into its operations.

- A diagram of the risk maturity cycle in its entirety can be seen at **Appendix A**, and is useful in gauging how the organisation is progressing in its risk management process.

1.3   Approach

The following approach was used in order to complete this review:

- Discussions were held with the Management Team to document the systems in place regarding risk management processes within the organisation;

- An evaluation of mitigating controls against risks was performed in order to identify key controls and areas for testing;

- Testing was performed on a sample basis on all key controls identified.

Section 1 - Executive summary (continued)

1.4   **Conclusion**

The following table details our overall assessment of the control environment against each audit objective:

Objectives	Overall Assessment	Report Ref.
A risk management strategy is in place for CNPA and is available across the organisation	****	
The process of risk management is consistent in all areas of CNPA	***	**2.2**
Personnel at all levels of CNPA are aware of the risk management process	***	**2.1**
A risk register has been created that identifies all major risks to the organisation	****	
The risk management process facilitates the effective reporting of risks to appropriate levels	****	
Action plans have been created to address risks facing the organisation, including the identification of those responsible for the management of risks	****	
All risks are measured and reviewed on a regular basis	****	
The risk register is updated on a regular basis	****	

Key:	****	Arrangements accord with good practice and are operating satisfactorily (recommendations are in respect of minor matters).
	***	Adequate arrangements are in place, but certain matters noted as requiring improvement.
	**	Arrangements in place offer scope for improvement.
	*	Inadequate level of control and unacceptable level of risk.

Section 1 - Executive summary (continued)

1.4 Conclusion (continued)

We can conclude, on the basis of our fieldwork, that the risk management process within CNPA is generally adequate, with only minor issues noted for improvement. If it were to be placed within the IIA Risk Maturity Cycle, CNPA could be assessed to be between stages 3 and 4, risk defined and risk managed, which would indicate significant progress in the period of 18 months. A summary of these stages can be seen at **Appendix A**. The minor issues noted for improvement were as follows:

- The Project Officers do not use the Risk Register as a point of reference when performing risk assessments for projects. *(Recommendation 2.1)*;
- The Risk Register is reviewed on a quarterly basis by the Management Team. However, these fortnightly meetings have only been formally minuted 3 times in this financial year. *(Recommendation 2.2)*;

Our detailed findings and recommendations are within **Section 2** of this report. In total, we identified **two** recommendations as follows:

Description	Priority	Number
Major issues that we consider need to be brought to the attention of Management and the Audit Committee	1	0
Important issues which should be addressed by management in their areas of responsibility	2	0
Minor issues where management may wish to consider our recommendations	3	2
Key		2

1.5 Acknowledgements

We would like to take the opportunity to thank all of the CNPA staff involved in assisting us in this audit. The findings and recommendations in this report were discussed with the Head of Corporate Services at the conclusion of our fieldwork.

Section 2 - Detailed findings and recommendations

2.1   Expenditure Justification Risk Assessment

Finding	Recommendation	Rationale
All expenditure over £5,000 requires an Expenditure Justification Form to be completed. One aspect of this form is the risk assessment for the project relating to the funding application. Heads of Groups have acknowledged that Project Officers have demonstrated a lack of understanding when completing this section of the form and as a result, guidance notes are being prepared by the Finance Manager in completing this process. The Risk Register is not used by Project Officers as a source document when completing the Risk Assessment.	The Finance Manager should ensure that the use of the Risk Register is included in the guidance notes for Project Officers. Project Officers should also be made aware of the location of the Risk Register.	This will ensure that all key organisational risks are considered when each project is risk assessed.

Management Response		Responsibility/ Deadline	Priority
Recommendation agreed. We will seek to highlight the location of the latest version of the Strategic Risk Register the Expenditure Justification guidance notes.		Finance Manager / Head of Corporate Services March 2007	Three

Section 2 - Detailed findings and recommendations (continued)

2.2   Management Team Minutes

Finding	Recommendation	Rationale	
The Management Team meets on a fortnightly basis to discuss all matters arising within the organisation. They review the Risk Register each quarter. The Head of Corporate Services is responsible for ensuring that all meetings are minuted. However this is a task which has lapsed in recent months and only 3 meetings have been formally minuted in this financial year.	All Management Team minutes should be documented and posted to the shared network drive. If it is not possible for the Head of Corporate Services to complete this task, consideration should be given to delegating this to another member of staff.	A number of decisions are made at Management Team meetings, including review of the Risk Register. Minutes would be required in order to provide an appropriate audit trail of the decision making or review process.	
Management Response		**Responsibility/ Deadline**	**Priority**
Recommendation accepted. Notes of Management Team (MT) meetings were initially prepared as an internal communications tool, to ensure staff could, if they wished, keep themselves informed of business considered by MT. Staff feedback suggested that these notes should only be issued in cases where significant matters required to be highlighted, in order to streamline internal communication processes. However, the matter of MT notes providing audit trails around decisions is now noted. The Head of Corporate Services undertook to prepare these notes in order to not place a further strain on already stretched administration resources within the organisation and we will continue to review the best use of staff time in meeting this recommendation.		Head of Corporate Services / December 2006	Three

Section 3 - Statement of responsibility

Statement of Responsibility

We take responsibility for this report which is prepared on the basis of the limitations set out below.

The matters raised in this report are only those which came to our attention during the course of our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of internal audit work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices. We emphasise that the responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by internal audit should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all circumstances of fraud or irregularity. Auditors, in conducting their work, are required to have regards to the possibility of fraud or irregularities. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud. Internal audit procedures are designed to focus on areas as identified by management as being of greatest risk and significance and as such we rely on management to provide us full access to their accounting records and transactions for the purposes of our audit work and to ensure the authenticity of these documents. Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system.

Deloitte & Touche LLP

Inverness

August 2006

In this document Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms and their respective subsidiaries and affiliates. As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms has any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte", "Deloitte & Touche", "Deloitte Touche Tohmatsu", or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the Deloitte Touche Tohmatsu Verein.

In the UK, Deloitte & Touche LLP is the member firm of Deloitte Touche Tohmatsu and services are provided by Deloitte & Touche LLP and its subsidiaries. Deloitte & Touche LLP is authorised and regulated by the Financial Services Authority.

Deloitte & Touche LLP is a limited liability partnership registered in England and Wales with registered number OC303675. A list of members' names is available for inspection at Stonecutter Court, 1 Stonecutter Street, London EC4A 4TR, United Kingdom, the firm's principal place of business and registered office.

Deloitte.

Risk Enabled (5)

Risk management and internal controls fully embedded into the operations
- Objectives are defined and management trained
- Scoring system for assessing risks
- Risk appetite in scoring system
- Processes for identifying and evaluating risks and responses implemented
- All risks brought together
- Specific responsibilities
- Monitoring processes and regular (quarterly) reviews
- All projects are risk assessed
- Management provide assurance to the Board

Risk Naïve (1)

No formal approach developed for risk management
- Objectives may be defined but management not trained
- No scoring system for assessing risks
- Risk appetite not defined
  Processes for identifying and evaluating risks and responses probably not defined
  Risks have not been identified nor brought together
- No specific responsibilities
- No monitoring processes nor regular reviews
- Projects are not risk assessed
- Management does not assure Board

Risk Aware (2)

Scattered silo based approach to risk management
- No consistent approach to defining objectives
- Limited management trained
- No consistent scoring system for assessing risks
- Risk appetite not defined
  Processes for identifying and evaluating risks and responses probably not implemented nor complete
- Some incomplete lists may exist without responsibilities
- Some monitoring processes and infrequent reviews
- Projects are not risk assessed
- Management does not assure Board

Risk Managed (4)

Enterprise approach to risk management developed and communicated
- Objectives are defined and management trained
- Scoring system for assessing risks
- Risk appetite in scoring system
- Processes for identifying and evaluating risks and responses implemented
- All risks brought together
- Specific responsibilities
- Monitoring processes and regular (quarterly) reviews
- All projects are risk assessed
- Some managers provide assurance to the Board

Risk Maturity Cycle

Risk Defined (3)

Strategy and policies in place and communicated. Risk appetite defined.
  Objectives are defined and management trained
- Scoring system for assessing risks
- Risk appetite in scoring system
  Processes for identifying and evaluating risks and responses implemented in some parts but not whole
  Risks brought together for some parts but not whole
- Specific responsibilities in some parts but not whole
  Monitoring processes and regular (annual) reviews
- Most projects are risk assessed
- Management does not assure Board

Deloitte.

Appendix B - Scope and objectives

Scope

We will undertake a review of the progress to date in further implementing a risk management system within the Authority, following our initial risk management workshop in 2004, and subsequent additions to the risk management system by the Director of Corporate Services.

Risk management is a key area for the Authority, not only in ensuring that all risks are managed to an acceptable level, but also in ensuring that the Chief Executive of the Authority can complete an unqualified statement in internal control within the annual accounts.

Objectives

With these factors in mind, our review will assess the controls in place to ensure that:

- A risk management strategy is in place for CNPA and is available across the organisation;

- The process of risk management is consistent in all areas of CNPA;

- Personnel at all levels of CNPA are aware of the risk management process;

- A risk register has been created that identifies all major risks to the organisation;

- The risk management process facilitates the effective reporting of risks to appropriate levels;

- Action plans have been created to address risks facing the organisation including the identification of those responsible for the management of risks;

- All risks are measured and reviewed on a regular basis; and

- The risk register is updated on a regular basis.

Appendix C - Personnel interviewed

- **David Cameron – Head of Corporate Service**

- **Fiona Newcombe – Head of Group,**

- **Nick Halfhide – Head of Group, Strategic Policy and Programme Management**

- **Murray Ferguson - Head of Group, Visitor Services**

- **Denby Pettitt – Finance Manager**

- **Andy Rinning – Head of Business Development**