Deloitte.

Cairngorm National Park Authority
Review of IT Contingency Planning
Internal Audit 2005/2006

March 2006

Strictly Private and Confidential

Deloitte.

Contents

Appendices

Deloitte.

Section 1 – Executive summary

1.1 Introduction

This review of Information Technology (IT) contingency planning is part of our coverage of operational areas as required in the audit plan approved by the Audit Committee. **Appendix A** shows the detailed scope and objectives of our review, which were agreed with the Director of Corporate Services prior ot the commencement of fieldwork.

1.2 Background

Contingency planning is about anticipating disastrous events and planning to cope with them. Contingency plans should be sufficiently detailed so that management and staff actually know what to do when disaster strikes. Modern day business depends upon the smooth functioning of interrelated systems, procedures, services and personnel. It is critical that plans are developed, tested and adopted in order to react to unexpected disruptions and to protect the Cairngorms National Park Authority (CNPA) in times of crisis. The loss of information technology and services can have a major impact, especially at CNPA, where significant reliance is placed upon this function.

The organisation has a single IT expert within the Corporate Services team, supported by the Head of Corporate Services and the Support Services Manager, who is responsible for managing and maintaining the organisation's IT environment. This environment, in general terms, consists of an electronic link between the Ballater and Grantown on Spey offices, with a further link being put in place to a second building within Grantown on Spey, operating a range of administration applications including MS Office for general usage and Outlook for internal and external email communication.

The organisation's main server is held within the computer room in the main Grantown on Spey office and remains under warranty with Dell Computers. In addition, the organisation holds maintenance/support contracts with the suppliers of the most critical equipment, including the British Telecom links between the offices as described above and the applications considered the most critical. The organisation also has a contract with "Primary Solutions" and the terms of this contract stipulate that they will provide support and assistance whenever there are instances where the functionality of the CNPA system is affected and where there is disruption in services. The organisation considers the most critical systems as the "Sage Financials" and "Sage Payroll" systems and the "Esri" mapping/planning system in use at the Ballater office. The Sage systems are considered critical in terms of managing the accounting process and for the payment of salaries whereas the Esri system is critical in enabling the organisation to meet its bi-weekly reporting obligations for the planning process.

1.3 Approach

The purpose of the review was to evaluate the organisation's capability to react to adverse situations that affect the functionality of the IT environment through effective contingency planning. Our approach to this audit was to document the processes and plans in place across the organisation and to establish the adequacy and effectiveness of the contingency planning arrangements. In particular, we sought to establish whether the organisation has adequate plans, resource and documentation to ensure that they can recover critical / vital systems in the event of any given disaster.

Deloitte.

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 Reference
There are adequate contingency plans, based upon the organisation's IT strategy and risk assessment process. Contingency plans should include: • Identification and prioritisation of systems and other resources required to support critical business processes in the event of a disruption (business impact analysis); • Appropriate strategies for recovery of at least sufficient IT facilities to support the critical business processes until such time as full facilities are available; and • Detailed plans for recovering IT facilities (disaster recovery planning).	**	**2.1, 2.2, 2.3**
Contingency plans are maintained (as the organisation changes and systems develop) and are regularly tested.	**	**2.1, 2.3**
Contingency plans support and link into the organisation's overall business continuity plan.	**	**2.3**

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.

Deloitte.

Section 1 - Executive summary (continued)

1.4 Conclusion (continued)

The organisation does not have any formal contingency plans in place. The extent of this exposure is somewhat mitigated by the maintenance/support contracts and systems warranties in place.

However, in overall terms, we conclude that the contingency planning arrangements are generally weak and there are a number of areas that the organisation should address. There are a number of control activities to implement in order to demonstrate that the organisation incorporates contingency planning within their activities and we have highlighted these controls at **Appendix B**.

The key areas of weakness are as follows:

- The organisation only has a "draft" overall business continuity plan. Consequently, it may not be sufficiently prepared to react to a major incident affecting the organisation. In addition, the development of individual IT contingency plans, to both support the overall plan and to recover important/critical systems, cannot be completed. *(Recommendation 2.1);*
- The organisation has not undertaken a risk assessment of the computing environment. Consequently, the organisation has not formally identified all risks (to hardware and software), assessing their likelihood and impact and identifying the actions necessary to reduce the risk exposure. *(Recommendation 2.2)*;
- There are a number of control activities that must be implemented in order for the organisation to demonstrate that contingency planning arrangements are adequate and effective. At present, there is limited contingency planning activity and therefore an inadequate state of readiness and an unnecessary exposure to risk. *(Recommendation 2.3)*.

Our detailed findings and recommendations are within **Section 2** of this report. In total, we identified **3** 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**	**3**
Minor issues where management may wish to consider our recommendations	**3**	**0**
Key		**3**

1.5 Acknowledgements

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

Deloitte.

Section 2 - Detailed findings and recommendations

2.1 CNPA business continuity plan

Finding	Recommendation	Rationale	
The organisation has produced a "draft" business continuity plan. This plan has not been subject to finalisation, formal approval and distribution.	The organisation should finalise and formalise the business continuity plan at the earliest opportunity.	Without an overall plan that is actually operational the organisation is exposed to the risk of inappropriate action should a major incident occur that disrupts the organisation's business activity. Only once the overall plan is finalised can the organisation commence the development of the IT contingency planning process that includes the identification of critical systems, minimal operating/processing requirements, risk assessment, testing of plans and actions taken to address areas of weakness/vulnerability.	
Management Response		**Responsibility/ Deadline**	**Priority**
Recommendation agreed.		Head of Corporate Services with Business Services and IT Managers, by end May 2006	Two

Deloitte.

Section 2 - Detailed findings and recommendations (continued)

2.2 Risk assessment

Finding	Recommendation	Rationale	
The organisation has not undertaken a risk assessment of the entire CNPA computing environment (across all locations). The CNPA risk register contains two entries for risks associated with any aspect of IT/telecoms. The two entries are the risks ranked #65 and #67 on the output from the risk workshop of 2004 that represents the organisation's risk register. The risks are "IT failure" and "exposure of IT systems to external attack", both with a low likelihood scoring/rating. These risks were identified at the workshop and not through a systematic IT-specific departmental – assessment, a process that the organisation is working towards.	The organisation should undertake a formal analysis and assessment of IT departmental risks and their potential impacts. This should be subject to regular review and updated to reflect changes in the computing environment over time. This could follow a eight step process as identified below: 1. Identify information assets (hardware and software). 2. Prioritise the assets identified. 3. Identify risks. 4. List and define the risks. 5. Prioritise risks. 6. Reference risks to critical assets. 7. Record all significant risks in the risk register. 8. Make recommendations and take actions to resolve the risks.	It is important that the organisation has a process in place to identify assets and their risks, determine the extent of the likelihood and impact of the risks and identify how the risks can be mitigated. Once risks have been identified, it is up to the organisation to determine if the extent of risk can be managed or if action should be taken to protect information assets.	
Management Response		**Responsibility/ Deadline**	**Priority**
Recommendation agreed. Timetable for action relates to completion of steps 1 to 7 of recommendation, with separate timetable for action plan to be determined thereafter.		Head of Corporate Services with Business Services and IT Managers, by end June 2006	Two

Deloitte.

Section 2 - Detailed findings and recommendations (continued)

2.3 Control environment

Finding	Recommendation	Rationale	
There are a number of control activities for the organisation to implement in order to be able to demonstrate that an adequate and effective contingency planning process is in place. At **Appendix B**, we provide a table that lists the steps and controls that we recommend the organisation should implement in order to be able to demonstrate that an adequate and effective process is in place for contingency planning.	Management should implement the steps as detailed at **Appendix B**. These include the following: • Development of plans; • Testing plans; • Taking action to address areas of weakness / vulnerability; and • Controlling distribution and version control.	Without an adequate and effective contingency planning process, the organisation is at risk of exposure to inappropriate or insufficient action when a major incident occurs that affects the IT environment.	
Management Response		**Responsibility/ Deadline**	**Priority**
Recommendation agreed.		Head of Corporate Services with Business Services and IT Managers, by end June 2006	Two

Deloitte.

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.

March 2006

Deloitte.

Appendix A - Scope and objectives

Scope

In 2005 Audit Scotland undertook an overview exercise of computer services and raised a number of action points. One of the action points required the organisation to prepare and maintain formal business continuity plans.

The scope of this review was to assess whether adequate plans are now in place to ensure that critical IT applications and data can be recovered in the event of any given disaster.

Objectives

In support of this scope, the objectives of this review were as follows:

- There are adequate contingency plans, based upon the organisation's IT strategy and risk assessment process. Contingency plans should include:
  - Identification and prioritisation of systems and other resources required to support critical business processes in the event of a disruption (business impact analysis);
  - Appropriate strategies for recovery of at least sufficient IT facilities to support the critical business processes until such time as full facilities are available; and
  - Detailed plans for recovering IT facilities (disaster recovery planning).
- Contingency plans are maintained (as the organisation changes and systems develop) and are regularly tested.
- Contingency plans support and link into the organisation's overall business continuity plan.

Deloitte.

Appendix B - Control environment

The following table lists the expected key actions and controls necessary for the organisation to be able to demonstrate that they have an adequate and effective system in place for contingency planning. The organisation is currently at risk of exposure to inappropriate or insufficient actions should a major incident occur that affects the IT environment as none of the actions and controls listed is in place.

#	*Control title*	*Control description*
1	**An overall business continuity plan is in place.**	An organisation-wide high-level business continuity plan should be in place.
2	**A series of smaller IT contingency plans are in place to support the overall plan.**	Elements of the overall business continuity plan will relate to IT and telecoms and these should have their own plans to support the overall plan. These include contingency plans for the servers, the communication links and for each individual application that is deemed important/critical.
3	**Management have identified and maintain records of their critical systems.**	The organisation should maintain a formal record of its important/critical systems. These are informally considered as being the Sage Financials and Payroll systems, the ESRI mapping/planning software and database and the MS Office suite.
4	**A contingency / recovery plan is in place for each system identified as being critical.**	Individual system/application plans should include the IT contingency and recovery activities and also incorporate the departmental plans and actions should their system be unavailable for any disruptive length of time.
5	**A formal risk assessment process has identified all risks (likelihood and impact).**	Management should have undertaken a process where all risks and vulnerabilities have been identified, documented, scored (likelihood and impact) and action plans put in place to address them. The most significant risks should be added to the risk register.
6	**All significant IT risks have been added to the organisation's risk register.**	This should be in place to record all significant risks, including those relevant to IT.
7	**Corporate Services ratify all contingency / risk decisions and activities.**	Corporate Services should approve all contingency plans, testing, risk assessments and risk scoring. In addition, all amendments to plans should be approved here. The Head of Corporate Services should report to the Board on such matters.
8	**The overall contingency plan is tested on an annual basis and updated as required.**	The overall plan should be subject to testing at least once per year. The test results should be analysed and actions put in place to address weaknesses.
9	**All testing results are reported and monitored within Corporate Services and actions are delegated.**	Corporate Services review all testing outcomes, delegating actions where needed to address weaknesses and ensuring that the plans are both adequate and effective.

Deloitte.

Appendix B - Control environment (continued)

10	**Each individual IT and departmental contingency plan is subject to six-monthly testing.**	For each important/critical system the contingency plan should be tested every six months to ensure that it is up to date, adequate and effective. This covers both the IT element and also the departmental recovery plans actioned when the IT system is down. The results of testing should be reported to the Head of Corporate Services for the delagating of action to address areas of weakness.
11	**Each department operating a critical system has communicated their expected recovery time.**	Each department - finance, HR, planning - should communicate their expectations for recovery times to the IT department. This is necessary to ensure that appropriate strategies are in place for the recovery of at least the minimum processing requirements to support important/critical business processes until such time as full facitities are available.
12	**Each critical hardware element is fully insured against loss.**	Each critical item of hardware (not already within warranty) should be fully insured. (Vulnerabilities should be identified at the risk assessment stage).
13	**Contingency plans are treated as being controlled documents.**	All plans should be controlled documents and as such subject to version control. The IT Support Manager (and nominated alternate) should maintain a list of recipients and communicate all changes, maintaining a master document centrally.

Deloitte.

Appendix C - Personnel interviewed

David Cameron – Head of Corporate Services

Sandy Allan – IT Support Manager