CAIRNGORMS NATIONAL PARK AUTHORITY
Audit Committee Paper 3 24/03/06
FOR DISCUSSION

Cairngorm National Park Authority
Review of Server Security
Internal Audit 2005/2006

March 2006

Strictly Private and Confidential

This report and the work connected therewith are subject to the Terms and Conditions of the engagement letter between Cairngorm National Park Authority and Deloitte & Touche LLP. The report is produced solely for the use of the Cairngorm National Park Authority. Its contents should not be quoted or referred to in whole or in part without our prior written consent except as required by law. Deloitte & Touche LLP will accept no responsibility to any third party, as the report has not been prepared, and is not intended for any other purpose. This report is prepared on the basis of the limitations on Page 6.

We would like to draw to your attention that the matters raised in this report are only those identified through the use of the automated security analysis tool, SekChek. They are not necessarily a comprehensive statement of all the weaknesses that may exist or all the improvements that might be made. Our recommendations for improvements should be assessed by you for their full financial and operational impact and you must test the appropriateness of any systems changes prior to implementation. We take no responsibility for testing any system changes prior to implementation.

Deloitte.

Contents

Appendices

Section 1 – Executive summary

1.1 Introduction

This review of the security of the main Grantown server is part of our coverage of information technology (IT) areas as required in the audit plan approved by the Audit Committee. **Appendix A** shows the detailed scope and objectives of our review.

1.2 Background

The Cairngorm National Park Authority, in keeping with most modern organisations, is heavily dependent and reliant upon the use of information technology to conduct its day to day business. In particular, information technology plays a key role in facilitating and supporting the organisation's planning processes, together with its internal and external communications – much of which rely on Outlook email systems.

Whilst the organisation has a relatively small number of users it is important that industry-standard security controls and parameters are in place and that the organisation takes full advantage of the available security settings on their operating system to ensure the integrity and confidentiality of business-critical data.

The organisation's server room is based on the first floor of the Grantown on Spey office and appears to have adequate security and environmental controls. This room houses the organisation's main server (Dell Poweredge 2600 running MS Windows 2003) and this server was the focus of our review in determining the adequacy and effectiveness of user security settings.

1.3 Approach

Our scope and objectives for this review focussed on the security of the organisation's primary server utilising third party provided audit software (SekChek). The application evaluates computer security against international best practices and enables us to produce detailed reports identifying security weaknesses as well as assessing risk ratings, implications and suggested corrective actions. Security configurations are compared against best practice and other industry averages compiled from more than 50 different countries. A summary report of the SekChek analysis is given at **Appendix B**.

Whilst it should be noted that SekChek is third party software, Deloitte undertake regular audits of the SekChek headquarters and have a formal contract for services in place.

We would like to draw to your attention that the matters raised in this report are only those identified through the use of the automated security analysis tool, SekChek. They are not necessarily a comprehensive statement of all the weaknesses that may exist or all the improvements that might be made. Our recommendations for improvements should be assessed by you for their full financial and operational impact and you must test the appropriateness of any systems changes prior to implementation. We take no responsibility for testing any system changes prior to implementation.

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
Utilising the third-party tool "SekChek" we reviewed the IT security parameters and controls over the main server and undertook the following: ➢ Analysis of system-wide security defaults and ALL user profiles on the system.	***	**2.1**
➢ Identification of security weaknesses, risk ratings, implications and suggested corrective actions.	***	**2.2, 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.

Section 1 - Executive summary (continued)

1.4 Conclusion (continued)

The output from the SekChek review shows that, overall, security on the organisation's main server is above average compared with other Windows 2000/2003 domains used in the Government sector.

However, there are some areas of weakness that could be strengthened as follows:

- The organisation has approximately 60 employees but there are 97 user accounts on the domain. Whilst a number of these may represent duplicate accounts (used when undertaking system administration duties) and guest and maintenance accounts the organisation should undertake a full review of the SekChek output to ensure that all accounts are valid and that user parameters are appropriate. *(Recommendation 2.1);*
- The password security settings are weak in that the majority of users can access the system with a blank password and the lockout parameters when attempting to access the system effectively enable a user to attempt access without restriction on the number of attempts. *(Recommendation 2.2).*
- The SekChek analysis identifies a number of highlights/comments in the findings section and management must ensure that each of these is given consideration with regard to taking action to address the issues arising. *(Recommendation 2.3).*

At **Appendix B**, we have reproduced the summary SekChek report that provides details of all highlights/comments and which identifies the main issues arising. In addition, the full SekChek report and supporting spreadsheet will be forwarded on to the organisation in order that the full findings and supporting data may be utilised when addressing recommendation 2.3 as identified above.

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.

Section 2 - Detailed findings and recommendations

2.1 Review of user access parameters

Finding	Recommendation	Rationale
The organisation has approximately 60 employees but there are 97 user accounts on the domain server. The organisation does not routinely review all user access rights and privileges.	Management should ensure that all user accounts are subject to an immediate review and subsequent reviews on at least a six-monthly basis.	Whilst a number of the accounts identified may represent duplicate accounts (for when undertaking system administration duties) and some guest and maintenance accounts a review of all privileges will ensure that all accounts are valid and that user parameters are appropriate.

Management Response	Responsibility/ Deadline	Priority
Recommendation Agreed.	Business Services and IT Manager / end April 2006	Two

Section 2 - Detailed findings and recommendations (continued)

2.2 Password security

Finding	**Recommendation**	**Rationale**	
The SekChek analysis output identifies the following issues regarding password security settings: • 69 users are allowed to log on with a zero length password. (Note that the ability to log on with a blank password may be overridden if the settings within the "password complexity policy" prevent this). • The "Lockout Threshold" parameters in the "Account Lockout Policies" are set such that a user has five attempts to log on to the system, after which they are locked out for ten minutes before another five attempts to log on are possible.	Management should ensure that all users are required to provide a password for each log in and that the "lockout duration" is set to 0 within the accounts policy after five unsuccessful access attempts have been made.	In general, allowing the use of null passwords is a *very high security risk,* because it will allow any person in possession of a valid account name to gain access to the system and information resources. However, there may be some special situations where it is appropriate for null passwords to be assigned to *some* special accounts (e.g. anonymous access with minimal privileges). The Lockout Duration should be set to 0 (forever) in the Accounts Policy to ensure that accounts are locked when the lockout threshold is exceeded and can only be unlocked by administrators.	
Management Response		**Responsibility/ Deadline**	**Priority**
Recommendation Agreed.		Business Services and IT Manager / end April 2006	Two

Section 2 - Detailed findings and recommendations (continued)

2.3 Action on SekChek findings

Finding	Recommendation	Rationale
The SekChek analysis output identifies a number of findings, both strengths and weaknesses. The weaknesses include the following: • 9 accounts have security administration privileges; • 25 accounts have not been used in the last 90 days; • 22 accounts have not changed their password in the last 90 days; and • 19 users are not required to change their passwords.	Management must ensure that there is a review of all the SekChek findings and that there are actions taken to address the issues. A summary of the key findings (with the actions required by CNPA) is reproduced at Appendix B and within the full and complete SekChek report distributed to the Head of Corporate Services.	All potential security weakness should be addressed in order to minimise the risk of exposure and security breaches.

Management Response	Responsibility/ Deadline	Priority
Recommendation agreed. In discussion between Head of Corporate Services and Deloitte, it has been agreed that this recommendation, while still highlighted as priority 2, is the least urgent of the 6 recommendations highlighted in both this and the Contingency planning report. Main findings of the SekChek report are already highlighted in recommendations 2.1 and 2.2 of this report. Timing of the deadline for this action is therefore slightly delayed from that of other IT recommendations.	Business Services and IT Manager / end October 2006	Two

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

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.

Appendix A - Scope and objectives

Scope

Adequate and effective security is a basic requirement for every networked IT system. There are many underlying components including firewall, routers, internet, access rights, virus protection etc. It is important that the organisation is suitably protected against security threats and that there are no major exposures.

In this, the second year of our provision of internal audit services, we focussed on the rights and controls governing the organisation's staff that access and work on the systems and applications maintained on the organisation's main computer server.

In future years we will concentrate on other aspects of security as the organisation expands and then formulates and implements information technology strategies.

Objectives

Utilising the third-party tool "SekChek" we reviewed the IT security parameters and controls over the main server and undertook the following:

- Analysis of system-wide security defaults and ALL user profiles on the system;
- Identification of security weaknesses, risk ratings, implications and suggested corrective actions.

Appendix B - Summary of SekChek findings

The following table is a reproduction of the summary report received from SekChek with a column added to identify the action required by CNPA, reference to recommendation 2.3.

Report Section	***Comments***	***Action required by CNPA***
-	The network does not have the latest Service Pack for Windows installed. The latest is SP1.	Review configuration and assess the benefits to be gained from updating the service pack
3	System Policy settings are generally OK. However: • The client could consider renaming the Administrator and Guest accounts. See comment 14 also.	For consideration.
4.1	The client is making some use of auditing features.	Review the auditing features not being used and determine if there is benefit to be gained from implementing them.
5	You should check the policies defined in the Group Policy Objects to ensure they are appropriate.	These relate to account permissions – for example password and defaults policies – and are the underlying permission settings..
7	In general, accounts are clearly assigned to specific people. 9 accounts have security administration privileges.	Establish if the 9 accounts with security administration privileges are appropriate.
9	Note that 3 accounts from trusted domains are members of local groups. These accounts will acquire the privileges of the local groups they belong to.	Review for appropriateness.
12	*SekChek* shows that 26% (25) of accounts have not been used in the last 3 months. Some of these may be redundant. This should be OK for service accounts. *NOTE:* *The domain being analysed has more than one domain controller. For this reason, you should not place reliance on the accuracy of the Last Logon Date. Use the information as a guideline only.*	Review the redundant accounts and remove them if they are no longer required or likely to be used in the short-term.

Appendix B - Summary of SekChek findings (continued)

Report Section	*Comments*	*Action required by CNPA*
13	Passwords for 23% (22) of accounts have not been changed in the last 3 months. This should be OK for service accounts.	The accounts should be reviewed and deleted if they are no longer required. Otherwise, their password change interval should be brought in line with installation standards. A generally accepted standard is to force users to change their passwords every 30 to 60 days. Some service accounts normally do not have their passwords changed frequently. For those accounts, the account name and password should be such that they are very difficult to guess.
14	20% (19) of users are not required to change their passwords due to settings at account level. Note that these settings override the client's Policy settings (see comment 3). This should be OK for service accounts.	Password change intervals for these user accounts should be brought in-line with the installation standard. A generally accepted standard for a password change interval is between 30 and 60 days. You should also check the Accounts Policy to confirm that the ***Maximum Password Change Interval*** is set to an acceptable value. Some service accounts normally do not have their passwords changed frequently. For those accounts, the account name and password should be such that they are very difficult to guess.
15	71% (69) of users are allowed to logon with a zero length password due to security settings in individual user accounts. See the report for implications and a detailed explanation.	In general, you should ensure strong passwords are assigned to all user accounts defined on your system. A generally accepted standard for a minimum password length is 6 characters.

Appendix B - Summary of SekChek findings (continued)

Report Section	*Comments*	*Action required by CNPA*
18	8 accounts, including the Guest account, are disabled.	Review the appropriateness of the accounts, removing if they are no longer required.
21.5	Some powerful rights are assigned to accounts other than those with security administration privileges.	Review all user rights for appropriateness.
22	The client should check that the listed permissions over objects are appropriate and in line with users' job functions.	Review all user rights for appropriateness.
23	The domain analysed has trust relationships with 1 other domain. *Note that security on the domain analysed is very dependent on the quality of security (particularly user authentication controls) on the trusted domain also.* *Similarly, security on the trusting domain is very dependent on the quality of security on the domain analysed.*	N/A This is the link with the server at Ballater.
26	No accounts can be used to dial-in to the domain via RAS.	N/A
27	The system seems to be running the Symantec (service was running) anti-virus software.	N/A
30	The system is using the NTFS file system.	N/A

Appendix C - Personnel interviewed

David Cameron – Head of Corporate Services

Sandy Allan – IT Support Manager