KPMG

cutting through complexity

Cairngorms National Park Authority

Internal audit report 2013-14

Review of IT general controls

19 February 2014

Contents

This report is for:

Action

David Cameron, *Corporate Services Director*

Information

Audit committee

Notice: About this report

This Report has been prepared on the basis set out in our Engagement Letter addressed to Cairngorms National Park Authority ("the Client") dated 15 June 2011 (the "Services Contract") and should be read in conjunction with the Services Contract. Nothing in this report constitutes a valuation or legal advice. We have not verified the reliability or accuracy of any information obtained in the course of our work, other than in the limited circumstances set out in the Services Contract. This Report is for the benefit of the Client only. This Report has not been designed to be of benefit to anyone except the Client. In preparing this Report we have not taken into account the interests, needs or circumstances of anyone apart from the Client, even though we may have been aware that others might read this Report. We have prepared this report for the benefit of the Client alone. This Report is not suitable to be relied on by any party wishing to acquire rights against KPMG LLP (other than the Client) for any purpose or in any context. Any party other than the Client that obtains access to this Report or a copy (under the Freedom of Information (Scotland) Act 2002, through the Client's Publication Scheme or otherwise) and chooses to rely on this Report (or any part of it) does so at its own risk. To the fullest extent permitted by law, KPMG LLP does not assume any responsibility and will not accept any liability in respect of this Report to any party other than the Client. In particular, and without limiting the general statement above, since we have prepared this Report for the benefit of the Client alone, this Report has not been prepared for the benefit of any other central government body nor for any other person or organisation who might have an interest in the matters discussed in this Report, including for example those who work in the central government sector or those who provide goods or services to those who operate in the sector.

Introduction and background

The contacts at KPMG in connection with this report are:

Stephen Reid

Director, KPMG LLP

Tel:	0131 527 6795
Fax:	0131 527 6666

stephen.reid@kpmg.co.uk

Brian Curran

Senior Manager, KPMG LLP

Tel:	0141 300 5631
Fax:	0141 204 1584

brian.curran@kpmg.co.uk

Ross Clarke

Audit Assistant, KPMG LLP

Tel:	0141 300 5521
Fax:	0141 204 1584

ross.clarke@kpmg.co.uk

Introduction and scope

Following discussions with management, we have agreed a change to the internal audit plan to perform a review of IT general controls, substituting the review of planning processes and systems.

Our review was designed to assess the design, implementation and operating effectiveness of a sample of IT general controls.

Background

The Cairngorm National Park Authority (‘CNPA’) utilises a number of computer programs including SAGE for finance functions, Snowdrop for HR functions and Microsoft Office in the day to day running of the organisation. The bulk of access is through Active Directory with SAGE having additional login requirements for finance staff.

Ultimate responsibility for information security lies with the Director of Corporate Services; at an operational level, this responsibility has been delegated to the IT Manager.

IT systems and software at the Authority are generally acquired off-the-shelf as readily available packages, for example, Microsoft Office and SAGE. IT hardware and software support is provided by various third party suppliers, when required.

This review has been conducted taking into account best practice from across the public sector and information security standard ISO 27001:2005, the international best practice standard for Information Security Management Systems.

Executive summary: Key findings and recommendations

We identified no 'critical' or 'high' risk graded recommendations in the course of our work.

We identified three 'moderate' risk and two 'low' risk graded recommendations

The findings identified during the course of this internal audit are summarised below. A full list of the findings and recommendations are included in this report. Management has accepted the findings and agreed reasonable actions to address the recommendations.

	Authority	Critical	High	Moderate	Low
Number of internal audit findings	CNPA	-	-	3	2
Number of recommendations accepted by management	CNPA	-	-	3	2

Summary of findings

We identified no 'critical or 'high' risk recommendations during this review. Recommendations identified relate to:

- tracking of adherence to software license agreements;
- timely completion of leavers and movers forms; and
- physical access to the server room.

Areas of good practice

Based on the sample testing undertaken, we noted that:

- password criteria are in line with best practice;
- backups of system data are taken on a regular basis and stored appropriately;
- control over the extension or purchase of new software licenses are robust, requiring a business case to be produced; and
- a copy of staff passwords are held in a locked safe in finance to avoid over dependence on a single employee.

Action plan

The action plan summarises specific recommendations, together with related risks and management's responses.

Finding(s) and risk	Recommendation(s)	Agreed management actions
1 System leavers and movers		**Moderate**
When a staff member leaves or moves roles within the organisation, a leavers form should be completed and provided to IT. It was found that forms are not submitted on a regular basis to ensure timely action by IT. There is a risk that staff leaving the organisation will not have their access disabled in a timely manner, leading to a potential security risk. Timely submission of leavers forms ensures that staff members leaving the Authority have their access disabled in a timely manner, and that staff moving roles do not have inappropriate access.	Management should ensure that leavers and movers forms are completed and processed in a timely manner.	Agreed. **Responsible officer**: Head of Organisational Development **Implementation date**: 30 June 2014
2 Software licences		**Moderate**
Software licences are purchased from companies such as Adobe and Microsoft to allow the organisation use of various products. It is important that the Authority adheres to the requirements of licence agreements. These may specify, for example, a maximum number of installations or a maximum number of users. It was found that IT staff are aware of these clauses and informally track adherence with them. However, there is no formalised documentation of this data, detailing the staff who have access to the software, the machines which have had it installed or the limits the organisation must comply with. There is a risk that compliance with the license agreements may be compromised or the need to alter a licence is not captured in a timely manner.	Management should: ■ maintain a spreadsheet of all the relevant data, ensuring a formalised approach to documenting adherence to the software licences; and ■ ensure this data is regularly reviewed for any issues or potential need for a reassessment of the license agreements.	Agreed. **Responsible officer**: Governance and Information Manager **Implementation date**: 30 June 2014

Action plan (continued)

Finding(s) and risk	Recommendation(s)	Agreed management actions
3 Disaster recovery procedure		**Moderate**
There is currently no formally approved disaster recovery procedure at the Authority. There is a risk that in the event of a failure of IT systems, management and operational activities would be negatively impacted.	Management should ensure that the disaster recovery procedure document is approved appropriately and published.	Agreed. There is a disaster recovery process now in place. However, we recognise that this has never been set out formally in a disaster recovery procedure which has been formally signed off by senior management. **Responsible officer**: Governance and Information Manager with IT Manager **Implementation date:** 30 June 2014
4 Server room physical access		**Low**
It is important that key IT equipment such as the server room is kept secure at all times. It was found that the server room is not kept locked at all times, leading to a risk of unauthorised access and/or damage to the Authority's servers.	Management should ensure that the server room is kept securely at all times.	Agreed. Although we note that the server room is located in a position with very little public access and risks associated are therefore significantly reduced. We will implement a locked server room process and have keys allocated securely **Responsible officer**: IT Manager **Implementation date**: 30 September 2014

Action plan (continued)

Finding(s) and risk	Recommendation(s)	Agreed management actions
5 Super user access		**Low**
Super users are individuals with unrestricted access to the IT systems. It is important for management to ensure the list of users that have this access to ensure that it is appropriate. There is one super user, but there is potential for some delegation to other individuals, thereby leading to more individuals with this access. There is currently no formal review by management over super user access rights, which may lead to a risk of an individual holding access that is no longer appropriate to the circumstances. This will be particularly relevant going forward if the size of the IT team is increased.	Management should review super user access to ensure access rights are appropriate.	Agreed. **Responsible officer**: Head of Organisational Development **Implementation date**: 30 November 2014

Appendices

Appendix one

Objective, scope and approach

Following discussions with management, we have agreed to make a change to the internal audit plan and to perform a review of IT general controls in place of the review of planning processes and systems.

Objective

The objective of this audit will be to review and test the processes and procedures in relation to IT general controls.

Scope

Based on the objective above we will focus on reviewing the design, implementation and operating effectiveness of controls in relation to: :

- software licence controls;
- back-up and recovery procedures;
- security of systems, including anti-virus controls and physical security;
- network security, including intrusion detection and prevention; and
- system administration rights control.

Approach

We will adopt the following approach to this review:

- project planning and scoping.
- conduct interviews with staff to gain an understanding of the Authority’s processes and procedures in relation to financial management, planning and efficiencies;
- identify and agree key risks and processes with management.
- review the adequacy and effectiveness of key processes through sample testing and discussion.
- agree findings and recommendations with management.

Classification of internal audit findings

The following framework for internal audit ratings has been developed and agreed with management for prioritising internal audit findings according to their relative significance depending on their impact to the process.

Rating	Definition	Examples of business impact	Action required
Critical	Issue represents a control weakness, which could cause or is causing severe disruption of the process or severe adverse effect on the ability to achieve process objectives.	■ Potential financial impact of more than 1% of total expenditure. ■ Detrimental impact on operations or functions. ■ Sustained, serious loss in brand value. ■ Going concern of the organisation becomes an issue. ■ Decrease in the public's confidence in the Authority. ■ Serious decline in service/product delivery, value and/or quality recognised by stakeholders and customers. ■ Contractual non-compliance or breach of legislation or regulation with litigation or prosecution and/or penalty. ■ Life threatening.	■ Requires immediate notification to the Authority's audit committee. ■ Requires executive management attention. ■ Requires interim action within 7-10 days, followed by a detailed plan of action to be put in place within 30 days with an expected resolution date and a substantial improvement within 90 days. ■ Separately reported to chairman of the Authority's audit committee and executive summary of report.
High	Issue represents a control weakness, which could have or is having major adverse effect on the ability to achieve process objectives.	■ Potential financial impact of 0.5% to 1% of total expenditure. ■ Major impact on operations or functions. ■ Serious diminution in brand value. ■ Probable decrease in the public's confidence in the Authority. ■ Major decline in service/product delivery, value and/or quality recognised by stakeholders and customers. ■ Contractual non-compliance or breach of legislation or regulation with probable litigation or prosecution and/or penalty. ■ Extensive injuries.	■ Requires prompt management action. ■ Requires executive management attention. ■ Requires a detailed plan of action to be put in place within 60 days with an expected resolution date and a substantial improvement within 3-6 months. ■ Reported in executive summary of report.

Classification of internal audit findings (continued)

Rating	Definition	Examples of business impact	Action required
Moderate	Issue represents a control weakness, which could have or is having significant adverse effect on the ability to achieve process objectives.	■ Potential financial impact of 0.1% to 0.5% of total expenditure. ■ Moderate impact on operations or functions. ■ Brand value will be affected in the short-term. ■ Possible decrease in the public's confidence in the Authority. ■ Moderate decline in service/product delivery, value and/or quality recognised by stakeholders and customers. ■ Contractual non-compliance or breach of legislation or regulation with threat of litigation or prosecution and/or penalty. ■ Medical treatment required.	■ Requires short-term management action. ■ Requires general management attention. ■ Requires a detailed plan of action to be put in place within 90 days with an expected resolution date and a substantial improvement within 6-9 months. ■ Reported in executive summary of report.
Low	Issue represents a minor control weakness, with minimal but reportable impact on the ability to achieve process objectives.	■ Potential financial impact of less than 0.1%*of total expenditure. ■ Minor impact on internal business only. ■ Minor potential impact on brand value. ■ Should not decrease the public's confidence in the Authority. ■ Minimal decline in service/product delivery, value and/or quality recognised by stakeholders and customers. ■ Contractual non-compliance or breach of legislation or regulation with unlikely litigation or prosecution and/or penalty. ■ First aid treatment.	■ Requires management action within a reasonable time period. ■ Requires process manager attention. ■ Timeframe for action is subject to competing priorities and cost/benefit analysis, eg. 9-12 months. ■ Reported in detailed findings in report.

KPMG

cutting through complexity