INTERNAL AUDIT SERVICES

REPORT REF No 2016/17 - 002

Loch Lomond & The Trossachs National Park Authority

General ICT Controls

November 2016

INDEX OF CONTENTS

Personnel associated with the report

Catriona Morton: Financial Performance Manager (Loch Lomond & The Trossachs National Park Authority)

Stevie Thomson: ICT Manager (Loch Lomond & The Trossachs National Park Authority)

Iain Kerr: ICT Security Officer (West Dunbartonshire Council)

1. AUDIT REPORT SUMMARY

1.1 General

An audit was conducted on General ICT Controls and we are pleased to report that the systems examined are working effectively.

The review highlighted that opportunities exist to strengthen internal controls and enhance the service provided, the most important of which are listed below:

- Enhance security at initial sign on by increasing the complexity of the Active Directory password;
- Introduce a more regimented approach to patching non Microsoft hardware/software; and
- Review the main IT security policy.

The Audit also highlighted areas of good practice as follows:

- An effective reciprocal arrangement with Cairngorms National Park Authority for (Disaster Recovery) DR and backup/recovery; and
- An effective, simple, dashboard to manage Anti-Virus/malware, Internet filtering and removable media.

Full details of these opportunities and any other points that arose during the audit are included in the Action Plan, which forms Section 3 of this report.

2. MAIN REPORT

2.1 Introduction

An audit was carried out on General ICT Controls as part of Internal Audit's Planned Programme of Audits for 2016/17.

2.2 Scope and Objectives

2.2.1 An audit launch meeting was held with Catriona Morton, Stevie Thomson and Iain Kerr to agree the objectives of the audit, the scope was signed off by Jaki Carnegie, Director of Corporate Services for Loch Lomond & The Trossachs National Park Authority (the Authority) consisting of:

- Review of Active Directory/Access controls, including password policy and GPO management;
- Review of Messaging controls, including Email policy, possibly covering Guest access;
- Review of Internet controls, including public interaction with web site and potential for compromise;
- Review of DR and Backup arrangements;
- Evidence of server and communication equipment Build documents;
- Review of Acceptable Use Policy and any other relevant policies;
- Review of Anti-Virus/malware protection;
- Evidence of PC build controls;
- Review of technology used for Remote workers, including remote access controls;
- Evidence of MOU's (or similar agreement)with partner organisations (Cairngorms National Park);
- Review of Handling of personal/sensitive information guidelines if relevant;
- Evidence of Patching routines/policies;
- Discussion on Intrusion prevention/detection, whether required;
- Review of Software licencing management; and
- Discussion on Penetration Testing, whether required.

2.2.2 Policies procedures and build documents were reviewed, the following is a list of relevant documents:

- Data agreement with Cairngorms;
- PC Build;
- DR Documentation;
- Enterprise Agreement;
- Imaging Documentation;
- ICT Policy;

- Example of Remote Access Authorisation Request;
- Back Up Diagrams;
- Back Up Schedule;
- Creating User Accounts; and
- Starter/Leaver procedures.

2.2.3 A detailed Audit response questionnaire was submitted in advance of the audit meeting with questions expanded and minute of responses agreed.

2.2.4 Demonstrations of key systems and processes were provided during the course of the Audit meeting.

2.2.5 Further evidence of controls required to access systems holding Personal/Sensitive information was provided.

2.3 FINDINGS

The findings are based upon evidence obtained from sampling/substantive testing.

2.3.1 The audit was conducted in conformance with the Public Sector Internal Audit Standards (PSIAS).

2.3.2 This report details all points arising during the audit review, full details of which are included in the Action Plan contained within Section 3 of this report. We stress that these are the points arising via the planned programme of work and are not necessarily all of the issues that may exist.

2.3.3 The factual accuracy of this report has been verified by the Officers involved in the audit.

2.3.4 All systems in the Authority are initially accessed via Microsoft's Active Directory network system, Active Directory has the capacity to enforce different levels of password complexity, with the current level set relatively low. The integrity of the Authority's systems would be better protected by increasing the initial sign on passwords complexity.

2.3.5 The audit established that overall the Policies, Procedures and build documents are robust and cover the areas that should be covered comprehensively. Following the review of the policies, in particular the main ICT Policy, it was identified that this could be updated to reflect current and new circumstances.

2.3.6 Whilst the Auditor noted the effectiveness of patch management for Microsoft software and operating systems, utilising Windows Software Update System (WSUS), patching of non-Microsoft hardware and software such as Communications equipment and Firewalls was carried out on a more Ad Hoc basis, an opportunity exists to introduce a more regimented patching regime for non-Microsoft equipment.

2.3.7 The Authority has a well-established agreement with Cairngorms National Park Authority for elements of DR and Backup/ Recovery as well as elements of systems support, the effectiveness of the arrangement was apparent during a recent cyber incident.

2.3.8 The Auditor noted the effectiveness of the software dashboard used to manage Anti-Virus/malware, internet filtering and management of removable media.

2.3.9 Whilst there is no legislative requirement to run regular Penetration tests, it would be good practice to run these periodically. Discussion around the potential for running Penetration tests at some point in future were received positively.

2.3.10 Evidence was provided describing the increased security required to access systems holding Sensitive/Personal information (HR and Payroll systems).

2.3.11 Audit would like to thank all staff involved in the audit process for their time and assistance.

3. Action Plan

ICT General Controls – Action Plan					
Finding	**Recommendation**	**Priority**	**Management Comment**	**Manager Responsible**	**Date to be completed**
1. Password strength The initial active directory password complexity used to access core Park Authority systems is set relatively low	Active Directory password complexity parameters should be strengthened to protect the integrity of core Park Authority systems	Medium	Agreed. The password complexity will be increased	Stevie Thomson	30/11/2016
2. Patch Management Whilst Microsoft systems are patched effectively, other key components of the Infrastructure are patched on a more Ad Hoc basis	Effective policy and associated processes should be introduced to cover the patching of all hardware and software	Low	The public facing firewall is patched on an ad-hoc basis because it is not possible to patch this during core hours, therefore the current process is to patch when the opportunity arises. We will prepare a timetable that schedules patching of the firewall on a quarterly basis to ensure that this is part of routine maintenance	Stevie Thomson	30/11/2016
3. IT Policy Review The IT Policy was last reviewed in May 2015	Best practice is to review biennially or sooner if any major systems changes occur	Low	Agreed	Stevie Thomson	31/05/2017
4. Penetration Testing Whilst there is no legislative requirement for regular Penetration testing, it would be good practice to run such tests periodically	Consideration should be given to running periodic Penetration/ vulnerability tests	Low	We will research the options for penetration testing and ensure that budget allocation is provided for this as part of 2017/18 budget	Stevie Thomson	30/11/2017

Appendix 1. Priority Levels

Recommendations have timescales for completion in line with the following priorities

Priority	**Expected implementation timescale**
High Risk: Material observations requiring immediate action. These require to be added to the risk register of a Service (Council context).	Generally, implementation of recommendations should start immediately and be fully completed within three months of action plan being agreed
Medium risk: Significant observations requiring reasonably urgent action.	Generally, complete implementation of recommendations within six months of action plan being agreed.
Low risk: Minor observations which require action to improve the efficiency, effectiveness and economy of operations or which otherwise require to be brought to the attention of senior management.	Generally, complete implementation of recommendations within twelve months of action plan being agreed.

Note: About this report

This Report has been prepared on the basis set out in the Memorandum of Understanding (MOU) between the Loch Lomond & The Trossachs National Park Authority as the Client and West Dunbartonshire Council (WDC) as the provider of Internal Audit services. 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 MOU. This Report has been prepared 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. This Report is not suitable to be relied on by any party wishing to acquire rights against WDC, 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, the Environmental Information (Scotland) Regulations 2004 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, WDC 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 public sector 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 public sector or those who provide goods or services to those who operate in the public sector.