

INTERNAL AUDIT SERVICES

REPORT REF No 2016/17 - 003

**Loch Lomond & The Trossachs
National Park Authority
Disaster Recovery/Business Continuity
Controls**



INDEX OF CONTENTS

Section	Contents	Page No.
1.	Audit Report Summary	3
	1.1 General	3
2.	Main Report	4
	2.1 Introduction	4
	2.2 Scope and Objectives	4
	2.3 Findings	5

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 Disaster Recovery/Business Continuity Controls and we are pleased to report that the systems examined are working effectively.

The review highlighted that robust Business Continuity arrangements are in place and ICT Disaster Recovery procedures are effective:

The Audit highlighted areas of good practice as follows:

- A comprehensive Business Continuity plan exists
- A comprehensive ICT Disaster Recovery plan exists
- An effective Disaster Recovery site has been established
- Both the Business Continuity and Disaster Recovery plans have been exercised recently with resulting reports and actions recorded

2. MAIN REPORT

2.1 Introduction

An audit was carried out on Disaster Recovery/Business Continuity 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, Paul Scullion, Jaki Carnegie, Colin McDougall 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:

The Business Continuity Plan

- Critical business partner relationships and stakeholder dependencies are identified and considered (including key suppliers, vendors, and outsourced functions);
- Does the Business Continuity Plan scope cover the entire operation, including all business processes and operations, as well as related facilities and workforce that are the responsibility of the Authority;
- All relevant entities and critical functions are considered within this Business Continuity Plan;
- Various types of events that could prompt the formal declaration of a crisis or disaster and the process for invoking the Business Continuity Plan are clearly described;
- The Business Continuity Plan includes impact and probability of disruptions of all business, operational, and IT areas, and considers acceptable downtime;
- Procedures exist to execute the plan's priorities for critical versus noncritical functions, services, and processes;
- Adequate risk mitigation, including preparedness and prevention strategies, have been considered, such as:
 - Alternative locations and capacity.
 - Back-up of data, applications, telecommunications, and other relevant data is ensured and procedures exist;
 - Communication channels in case of emergency are clearly defined; and
 - All critical personnel are identified and the contact list is updated.

Review/Testing

- The Business Continuity Plan is updated, reviewed, and tested at a frequency appropriate for risks, vulnerabilities, and value of Authority functions;
- Members of the Business Continuity Plan team understand their roles in case of emergency;
- Within the Business Continuity Plan, the Authority has set testing requirements for the continuity of services, functions, business lines, support functions;
- Conclusions regarding the testing program and whether it is appropriate for the size, complexity, and risk profile of the Authority are documented; and
- The Business Continuity Plan exercise details, such as content, participants, and timing are documented.

2.2.2 The following documents were reviewed as part of the Audit process:

- Business Continuity Plan;
- DR Documentation;
- ICT DR Exercise; and
- BCP Desktop Exercise Report.

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 A site visit to the main Disaster Recovery location and explanations of key systems and processes 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. 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 The Business Continuity Plan is a comprehensive document covering all expected aspects of such a plan and is a “live” document, changing as new scenarios come to light.

2.3.5 The Disaster Recovery plan is a comprehensive document covering all expected aspects of such a plan and is a “live” document changing to adapt to new and emerging threats.

2.3.6 The Disaster Recovery site has all the expected hardware and communication equipment to allow the authority to run in the event of a complete failure of ICT systems.

2.3.7 The capacity of the Disaster Recovery site has been considered by the Auditor and relevant staff, and all the Authority’s functions could operate from the DR site within the stated timescales, albeit slightly slower- this being a normal expectation for a DR site.

2.3.8 A “Battle box” at the Disaster Recovery site has all required documentation and equipment to re-establish the Authority’s systems

2.3.9 The Business Continuity plan was exercised recently using a flooding scenario with relevant staff considering challenges presented by the loss of the primary site for a lengthy time period. Recommendations for improvements were documented and a commitment to exercise annually agreed.

2.3.10 The Disaster Recovery Plan was exercised recently emulating a complete loss of the primary data centre and full recovery at the secondary site. Outcomes were documented and a commitment to exercise annually agreed.

- 2.3.11 Internal Audit would like to note the good practice of exercising both the Business Continuity Plan and Disaster Recovery plans annually.
- 2.3.12 Audit would like to thank all staff involved in the audit process for their time and assistance.

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.