Loch Lomond & The Trossachs National Park Authority

Business Continuity Planning

Final Report

AUDIT GLASGOW

March 2022

Glasgow
CITY COUNCIL

Loch Lomond & The Trossachs National Park Authority
Business Continuity Planning

Table of Contents

FS 57095
Management System Certification

Audit Glasgow
Loch Lomond & The Trossachs National Park Authority – Business Continuity Planning

Loch Lomond & The Trossachs National Park Authority
Business Continuity Planning

1.   Introduction

1.1   As part of the 2021/22 Internal Audit plan we have carried out a review of the business continuity planning arrangements within Loch Lomond & The Trossachs National Park Authority (the Park Authority).

1.2   Business continuity planning is intended to achieve the minimum of disruption to the processing of business critical systems from the effects of major failures or disasters. A Business Continuity Plan (BCP) should provide a well-defined set of procedures to be followed to maintain business-critical processing and to achieve recovery. A failure to develop effective BCPs could result in an inability to ensure that the business continues to operate should a major failure or a business-critical event occur. This could increase the Park Authority's exposure to a range of operational, financial and reputational risks.

1.3   The purpose of the audit was to provide assurance on the business continuity arrangements in place. This included ensuring that lessons learned from the response to the COVID – 19 pandemic had been considered. The scope of the audit included a review of:

- Business continuity planning policies, procedures and controls;
- Operational BCPs;
- BCP roles and responsibilities;
- Critical systems and processes determination controls;
- Recovery prioritisation procedures;

- Recovery Time Objectives, Recovery Point Objectives and Maximum Tolerable Period of Disruption processes;
- BCP testing; and
- Monitoring and reporting of business continuity planning issues.

The audit did not include a review of the IT disaster recovery arrangements and processes in place within the Park Authority.

2.   Audit opinion

2.1   Based on the audit work carried out a reasonable level of assurance can be placed upon the control environment. The audit has identified some scope for improvement in the existing arrangements and three recommendations which management should address.

3.   Main Findings

3.1   We are pleased to report that the key controls are in place and generally operating effectively. We found that an Incident Response and Business Continuity Plan (the Plan) covering the whole organisation is in place and this is regularly reviewed to ensure it remains fit for purpose. Business continuity planning arrangements have been reviewed and updated where required as a result of lessons learned from the COVID - 19 pandemic.   The current version of the Plan is in draft and is due to be finalised and approved once the findings from this audit have been actioned.

3.2   BCP roles and responsibilities are documented within the Plan and arrangements are in place to ensure that any business continuity related issues or changes are communicated to the relevant parties. The Operational

2

Managers Group made up of Executives and Operational Managers acts as the Incident Management Team when required and meet regularly when an incident occurs. Adequate arrangements are in place for cascading information in the event of an incident. There are appropriate monitoring and reporting mechanisms in place to provide senior management, the Audit and Risk Committee and the Board with updates on any issues in relation to business continuity.

3.3 However, our audit testing found that there are some areas where controls could be improved. Although we were advised that the Plan is stored securely, both electronically and hard copy, the locations where hard copies of the Plan are stored are not fully documented. The arrangements for escalating business continuity related issues are also not documented.

3.4 Although the Plan covers the Park Authority as a whole, there are no service area specific Business Impact Assessments (BIAs) in place. Maximum Tolerable Period of Disruption (MTPOD) times have been set in the event of an ICT disaster, however no Recovery Time Objectives (RTOs) or Recovery Point Objectives (RPOs) have been agreed.

3.5 The Plan is a confidential document and therefore its access is restricted to the officers who are included within the Plan. However, there is no other BCP related guidance available to the wider staff. BCP training is also currently not available to staff.

3.6 We found that a BCP testing schedule is not in place.

3.7 An action plan is provided at section four outlining our observations, risks and recommendations. We have made three recommendations for improvement. The priority of each recommendation is:

Priority	Definition	Total
High	Key controls absent, not being operated as designed or could be improved. Urgent attention required.	1
Medium	Less critically important controls absent, not being operated as designed or could be improved.	2
Low	Lower level controls absent, not being operated as designed or could be improved.	0
Service Improvement	Opportunities for business improvement and/or efficiencies have been identified.	0

3.8 The audit has been undertaken in accordance with the Public Sector Internal Audit Standards.

3.9 We would like to thank officers involved in this audit for their cooperation and assistance.

3.10 It is recommended that the Chief Internal Auditor submits a further report to the Audit and Risk Committee on the implementation of the actions contained in the attached Action Plan.

4. Action Plan

Title of the Audit: Loch Lomond & The Trossachs National Park Authority – Business Continuity Planning

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: Business critical processes have been identified and risks relating to these services have been considered				
1	Although an Incident Response and Business Continuity Plan (the Plan) is in place that covers the organisation as a whole, we found that no service area specific BIAs have been undertaken. The electronic Plan is held in a restricted folder that can only be accessed by relevant staff, however the locations where hard copies of the Plan are stored are not fully documented. The Plan also does not detail the process for escalating business continuity issues. We found that RTOs and RPOs in the event of an ICT disaster have not been agreed and documented. It is a good practice to ensure that RTOs (the amount of time an organisation has to restore its processes at an acceptable service level after a disaster to avoid intolerable consequences associated with the disruption) and RPOs (the maximum amount of data as measured by time that can be lost after a recovery from a disaster, failure or comparable event before data loss will exceed what is	Senior management should carry out service specific BIAs to inform BCP processes. RTOs and RPOs in the event of an ICT disaster should be agreed and documented. Thereafter, the Plan should be updated to ensure that it includes: • Guidance on the process for escalating business continuity related issues. • The locations of the hardcopy Plan. • Details of the agreed RTOs and RPOs. • Any relevant information resulting from the completion of the BIAs. The Plan should then be approved accordingly and made available to the relevant staff.	**High**	**Response:** Accepted We will consider where BIA's will have most impact and develop these as appropriate. RTO's and RPO's will be agreed and added to the BCP (tentative timescale for this subject to agreement with the ICT Manager). The BCP will also be updated to include the process for escalating issues, and the location of hard copies of the Plan. **Officer Responsible for Implementation:** Estates Manager **Timescale for Implementation:** BIA's/Process for escalation and location of plans – 30 September 2022 RTO's/RPO's – 31 December 2022

	acceptable to an organisation) are set as they help inform effective BCP strategies. This increases the risk that the Park Authority has not fully considered the impact that any loss or interruption to services may have and that relevant officers may not be fully aware of the current and correct processes to follow should a major failure or a business-critical event occur.				
Key Control: Appropriate BCP guidance and training has been provided to staff.					
2	The Plan is a confidential document and therefore its access is restricted to officers who are included within the Plan. However, there is no other business continuity guidance available to the wider staff. We were also advised that BCP training is currently not available to staff. This increases the risk that staff are not aware of their roles and responsibilities during a BCP event.	Senior Management should ensure that business continuity guidance is available to all staff. Consideration should be given to introducing BCP training, in particular for those officers who have specific BCP responsibilities.	**Medium**	**Response:** Accepted A short document which outlines the main provisions for any incidents will be developed and made available to all staff. All staff who have specific BCP responsibilities will be included in the BCP testing exercises. **Officer Responsible for Implementation:** Estates Manager **Timescale for Implementation:** 30 April 2022	

No.	Observation and Risk	Recommendation	Priority	Management Response
Key Control: BCPs have been regularly tested and action has been taken to revise plans based on the test findings.				
3	A desktop testing exercise (scenario-based) was last carried out in 2017, however no action was taken to revise the Plan based on the findings from this exercise. The Park Authority utilised it's BCP arrangements in response to the COVID – 19 pandemic and the BCP was updated to reflect any lessons learned from this 'live' event. However, there is currently no BCP testing schedule in place. This increases the risk that the Park Authority are unaware of the effectiveness of the BCP and should a BCP event occur, staff may be unequipped to implement the plan effectively.	The Park Authority should develop a testing schedule, ensuring that testing is carried out on at least an annual basis. It should also ensure that the BCP and other relevant associated documentation are updated to reflect any lessons learned. The lessons learned process should also be completed following live incidents. Monitoring arrangements for this testing schedule should be in place to ensure that the regular BCP testing is undertaken.	**Medium**	**Response:** Accepted A schedule for testing will be developed and commence 22/23 Financial Year, with the next test to be scheduled after a suitable period of time under our new hybrid working model (commencing 1/3/22). **Officer Responsible for Implementation:** Estates Manager **Timescale for Implementation:** 30 September 2022