Business Continuity

Peak District National Park Authority
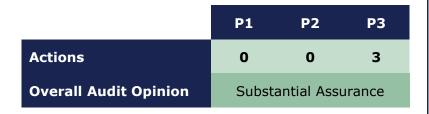
Internal Audit Report 2021/22

Business Unit: Various
Responsible Officer: Head of Information and Performance Management
Date Issued: 27 May 2022
Status: Final
Reference: 69146/002

	P1	P2	P3
Actions	0	0	3
Overall Audit Opinion	Substantial Assurance		

▲Veritau

Summary and Overall Conclusions

Introduction

Business continuity is the process of planning to ensure an organisation can continue with its operations in the event of a major incident such as fire, pandemic or loss of IT services. It is essential that a comprehensive and well implemented business continuity plan is in place to minimise the disruption to services and to ensure a timely recovery.

The Peak District National Park Authority has a corporate business continuity plan in place, which is supported by business impact assessments for each service. The Covid-19 pandemic has led to significant changes in working practices and there has been a corporate restructure resulting in changes to roles and responsibilities within the business continuity plan. Therefore, the audit has reviewed the plan to provide assurance that effective business continuity arrangements remain in place.

Objectives and Scope of the Audit

The purpose of this audit was to provide assurance to management that procedures and controls within the system will ensure that:

- Suitable management arrangements are in place for business continuity.
- Business impact assessments are complete and up to date, with critical functions identified and prioritised.
- There is a comprehensive and up to date business continuity plan in place to minimise service disruption.

The audit followed up actions agreed during the 2019-20 Business Continuity audit to confirm whether they had been completed. ISO 22301:2012 Business Continuity Management Systems and CIPFA guidance were used as good practice reference points during the audit.

Key Findings

The Peak District National Park Authority has a comprehensive corporate business continuity plan (BCP) in place, which sets out procedures for responding to an incident. Suitable management arrangements are in place: there is a senior nominated officer with responsibility for business continuity and each service has a designated officer with responsibility for business continuity in their area. There is a documented review schedule for the BCP and appendices and these are reviewed and updated regularly. The emergency contact list is updated every 6 months. The plan contains clearly defined and documented roles and responsibilities for during and following an incident as recommended in good practice guidance.

Business impact assessments (BIA) have been completed for each service and identify key functions and resource requirements. Heads of service have reviewed the BCP against their BIA and found that this meets the business continuity requirements for their services. There are no explicit recovery time objectives identified for key service functions in the BIAs, however, consideration is given to service restoration priorities in the BCP. Best practice guidance recommends the inclusion of recovery time objectives in BIAs to provide clear

minimum timeframes for restoration of key functions. The BIAs are currently being updated following the corporate restructure, however, there is no documented review schedule for BIAs.

The BCP contains documented procedures for activating and implementing the plan including an IT disaster recovery (DR) plan and testing arrangements. IT services are currently being migrated to new data centres. The migration is expected to be completed in May 2022 and a DR test will take place after that.

The management team discuss business continuity at leadership meetings and have recent experience of implementing the BCP. However, there are no formal arrangements in place for training or ensuring awareness of business continuity responsibilities for any member of staff.

Exercising of the plan has not been required in recent years because the plan was activated in response to the Covid-19 pandemic in 2020-21 and a bad weather event in 2018. The BCP requires that post-implementation reviews are completed to capture lessons learnt from activating the plan. A post-incident review is underway following Covid-19, but this has not yet been completed. Good practice guidance recommends that lessons learnt reviews are completed in a timely manner to prevent learning from incidents being lost.

The actions from the previous audit have been completed, with the plan now covering arrangements for volunteers during an incident.

Overall Conclusions

A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited. Our overall opinion of the controls within the system at the time of the audit was that they provided Substantial Assurance.

1 Lessons Learnt Reviews

Issue/Control Weakness	Risk
A post-incident review of lessons learnt from Covid-19 has not yet been completed.	If post-incident reviews are not completed in a timely manner, learning could be lost.

Findings

At the time of the audit, a post-incident review to capture lessons learnt from Covid-19 had not been completed. The Head of Information and Performance Management indicated that work was underway to do so. The authority's business continuity plan requires that learning from incidents is fed into improvements for planning and incident response. When the plan was activated in February 2018, a lessons learnt review was undertaken and presented to the senior leadership team in April 2018.

Best practice guidance, such as ISO 22301 section 9, recommends that post-incident reviews are conducted promptly to ensure learning is captured. This forms part of the 'Plan, Do, Check, Act' model ISO uses to promote continual improvement. Ensuring that the lessons learnt exercise is completed in a timely manner is important to ensure that learning from the activation of the business continuity plan during Covid-19 is not lost.

Agreed Action 1.1

A post-incident review from Covid-19 will be completed. The business continuity plan will be updated with any lessons learnt from the review.	Priority	3
	Responsible Officer	Head of Information and Performance Management
	Timescale	30 September 2022

Veritau

2 Business Impact Assessments

Issue/Control Weakness	Risk
Explicit recovery time objectives have not been identified for the key functions of services. A review schedule for business impact assessments is not included in the business continuity plan.	If recovery time objectives are not established and BIAs not kept up to date, incident response may be less effective or timely.

Findings

CIPFA and ISO 22301 section 8 recommend that business impact assessments (BIAs) include recovery time objectives for each service to assess the impact over time of not performing key functions. This assessment should consider the timeframe at which point not resuming functions would become unacceptable to the organisation, thus exposing it to the risk of loss or other harm. This should allow for the development of prioritised timeframes for service restoration at the minimum acceptable level. BIAs should also be regularly updated and reviewed.

Review of a sample of five BIAs found that recovery time objectives had not been defined for key service functions. While the BIAs identified key elements such as processes, staff and resource requirements, only one recorded statutory timescales.

The business continuity plan contains a service restoration priority, identifying the order in which services should be restored. However, there are no explicit minimum timeframes for resuming key service or consideration of the impacts of not doing so in these timeframes. Inclusion of recovery time objectives in the BIAs could help inform service restoration priorities in the business continuity plan, providing clear minimum timeframes for restoration for all key functions.

The BIAs are currently being updated following organisational changes but are not included in the review schedule in the business continuity plan. An annual review schedule including the business impact assessments would ensure their regular review and support updates to the business continuity plan based on the findings of the business impact assessments.

Agreed Action 2.1

Recovery time objectives will be developed for business impact assessments. The business continuity plan will be updated to include business impact assessments in the annual review schedule.	Priority	3
	Responsible Officer	Head of Information and Performance Management
	Timescale	30 September 2022

Veritau

3 Business Continuity Training

Issue/Control Weakness	Risk
No formal training is provided on business continuity	If staff are not trained or aware of business continuity responsibilities, the response to an incident may be less effective or timely.

Findings

CIPFA guidance and ISO 22301 section 7 highlight the role of training on business continuity to ensure relevant staff have the necessary awareness and competence in implementing, maintaining and continually improving business continuity planning. The Authority discusses business continuity and lessons learned at leadership meetings, which provides awareness of business continuity responsibilities to those staff. The management team also have recent experience of implementing the plan during Covid-19.

While the management team would primarily be responsible for implementing the business continuity plan in response to an incident, all staff have a role in the response. In particular, there are currently no arrangements in place to provide awareness for all staff on the responsibilities involved in the first responder role, which could impact an initial incident response. Any member of staff may be the first to discover an incident and so it is important that they understand their responsibilities during the initial response period.

Furthermore, the previous officer at the Authority with responsibility for business continuity had received formal training in this area. Roles in the organisation have now changed and this officer is no longer employed at the authority. The current officer with this responsibility has not received the formal business continuity training.

Agreed Action 3.1

The management team will assess staff training requirements, identify appropriate training and arrange for this to be completed.	**Priority**	3
	Responsible Officer	Head of Information and Performance Management
	Timescale	30 December 2022

Audit Opinions and Priorities for Actions

Audit Opinions

Our work is based on using a variety of audit techniques to test the operation of systems. This may include sampling and data analysis of wider populations. It cannot guarantee the elimination of fraud or error. Our opinion relates only to the objectives set out in the audit scope and is based on risks related to those objectives that we identify at the time of the audit.

Our overall audit opinion is based on 4 grades of opinion, as set out below.

Opinion	Assessment of internal control
Substantial Assurance	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable Assurance	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited Assurance	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

Priorities for Actions

Priority 1	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Priority 2	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Priority 3	The system objectives are not exposed to significant risk, but the issue merits attention by management.

▲Veritau