Appendix 3

Business Continuity

Peak District National Park Authority

Internal Audit Report 2019/20

Business Unit: Various
Responsible Officer: Senior Leadership Team
Date Issued: 17 October 2019
Status: Final
Reference: 69146/001

	P1	P2	P3
Actions	**0**	**0**	**2**
Overall Audit Opinion	High Assurance		

Summary and Overall Conclusions

Introduction

The Peak District National Park Authority (PDNPA) statutory responsibilities for business continuity are outlined in the Civil Contingencies Act 2004, which states 'local authorities should ensure that they can continue to deliver their functions in an emergency as far as is reasonably practicable'.

Business Continuity provides a framework, which identifies and outlines potential disruptions to the delivery of services provided by the Authority, and the responses to them. It is important a clear plan exists which outlines these procedures and processes. This plan will help to ensure critical services are back up and running as quickly as possible.

For authorities such as the Peak District National Park Authority, management of emergency scenarios without prior planning may result in adverse media coverage, loss of stakeholder confidence and impact on the statutory functions that the Authority carries out as well as increased overall costs.

Objectives and Scope of the Audit

- Essential business processes have been identified
- There are comprehensive Business Continuity plans in place to reduce the impact of service disruption
- Business Continuity plans are regularly monitored and kept up-to-date.

Key Findings

The Peak District National Park Authority have arrangements in place to reduce the impact of disruption to normal working conditions.

The Authority has a detailed corporate business continuity plan in place that set out the steps the leadership team should take in the event of service disruption, for example the loss of ICT and the Authorities offices. The plans covers all directorates within the Authority. The business continuity plan has been reviewed at least once a year since it was created in January 2016. However the business continuity plan does not include a protocol for how the Authority will contact and co-ordinate volunteers during disruption to services.

CIPFA and ISACA best practice guidance on business continuity recommends that organisations carry out a business impact assessment of all service areas to identify that all key personnel, assets and data have been identified and there is no points of failure within the service area. Through discussions with service managers, this is something that has not been carried out using a formal method. The guidance also recommends a business continuity plan for each service. Out of all the service departments, we had looked at only the democratic services &

legal team and the I.T team had one in place (This was so the head of the service had access to all of the contact details for Members). The heads of the other services that we spoke to felt that the corporate business continuity plan covered all key areas. It is also worth noting that many service departments within the Authority are non-critical and could continue to meet their objectives without access to the Authority's building and access to the ICT network for a limited period. A business impact assessment and service business continuity plan may not be required for all services due to the nature of their work, although this should be formally agreed at a corporate level.

The Authority's business continuity plan states that the plan will be tested every two years. The Authority has since taken the decision to carry out a lessons learned exercise following any time that the plan had been activated. The last time the plan had been activated was during April 2018 and there was a lessons learnt report produced following that incident. We have followed up on the report and found all the actions have been completed. Due to the geography of the Peak District, it is likely that the plan will be activated once every one to two years due to weather conditions and therefore regularly tested, although a formal test should be carried out if no incident occurs within a 2 year period. In addition to this, the Authority has also successfully tested the ICT disaster recovery plan in August 2018 to obtain assurance that the ICT network can be restored following a network outage.

Overall Conclusions

It was found that the arrangements for managing risk were very good. An effective control environment appears to be in operation. Our overall opinion of the controls within the system at the time of the audit was that they provided High Assurance.

1 Business Impact Assessments.

Issue/Control Weakness	Risk
Each service within the Authority has not carried out a business impact assessment.	Points of failure within the authority's functions have not been identified leading to a lack of contingency plans being put in place. This may lead to the authority being unable to deliver their goals during disruption to normal circumstance.

Findings

Before developing a business continuity plan CIPFA and ISACA best practice guidance states that a business impact assessment should be carried out for each service area. Business impact assessments (BIA) is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations because of a disaster, accident or emergency. The analysis can be used to identify points of failure within services. Once the assessment have been carried out, it can also be used to assess if any contingency plans would need to be implemented.

The authority did not carry out a formal business impact assessment for each service area before the corporate business continuity plan was created, although the creator of the business continuity plan did consult with the heads of service about whether the business continuity plan covered all key content for their service. A formal business impact assessment may provide detailed assurance that all of the authorities' business functions were reviewed and have sufficient contingency plans in place. A business impact assessment may not be required for all services due to the nature of their work, although this should be formally agreed at a corporate level

Agreed Action 1.1

During the creation of the corporate Business Continuity (BC) plan, each service did consider their key functions, and the impacts of any significant event. Though this analysis was not documented in a formal way, its findings were fed into the corporate BC plan.

The merits of completing this exercise retrospectively have been considered between Service Heads. Whilst there is a view that it is unlikely to lead to much alteration to the BC plan, it may be a helpful exercise and document set when staff changes take place at senior levels. These BIA's will help new staff in these roles understand the key functions and impacts clearly if a BC situation were to arise during the period of a new starter joining the Authority. To that end, we will complete service level BIA's as a part of the next review period for the BC Plan.

Priority	3
Responsible Officer	Head of Information Management
Timescale	April 2020

2 Business Continuity Plan- Volunteers

Issue/Control Weakness	Risk
The Authorities Business Continuity plan does not cover the co-ordination of volunteers.	Volunteers are not informed that business continuity plan has been activated and updated what actions to take.

Findings

The Authority has a comprehensive business continuity plan that covers the actions that the authority would take to respond to incidents and emergency contact details, and mitigation actions that the authority have in place.

However, the business continuity plan does not include anything in relation to contacting and coordinating volunteers during an incident. As the Peak District National Park Authority has around 600 volunteers that carry out a wide range of functions including conservation and project work there should be a plan of what actions to undertake in the event of an incident.

Agreed Action 1.2

Whilst the BC plan does have provision for volunteering activities, this could certainly be strengthened to include additional detail for contacting volunteers (above and beyond the current provisions for general public communication and liaison through volunteer leaders throughout the organisation).

The provisions for volunteering will be reviewed and updated as a part of the next BC review process.

Priority	3
Responsible Officer	Volunteer Coordinator
Timescale	April 2020

Audit Opinions and Priorities for Actions

Audit Opinions
Audit work is based on sampling transactions to test the operation of systems. It cannot guarantee the elimination of fraud or error. Our opinion is based on the risks we identify at the time of the audit. Our overall audit opinion is based on 5 grades of opinion, as set out below.

Opinion	Assessment of internal control
High Assurance	Overall, very good management of risk. An effective control environment appears to be in operation.
Substantial Assurance	Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified.
Reasonable Assurance	Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made.
Limited Assurance	Overall, poor management of risk with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation.
No Assurance	Overall, there is a fundamental failure in control and risks are not being effectively managed. A number of key areas require substantial improvement to protect the system from error and abuse.

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.

Where information resulting from audit work is made public or is provided to a third party by the client or by Veritau then this must be done on the understanding that any third party will rely on the information at its own risk. Veritau will not owe a duty of care or assume any responsibility towards anyone other than the client in relation to the information supplied. Equally, no third party may assert any rights or bring any claims against Veritau in connection with the information. Where information is provided to a named third party, the third party will keep the information confidential.