APPENDIX 3

MAIN ACCOUNTING

PEAK DISTRICT NATIONAL PARK AUTHORITY

INTERNAL AUDIT REPORT

	Critical	Significant	Moderate	Opportunity
Findings	0	0	1	0
Overall audit opinion	**Reasonable assurance**			

Status: Final

Date issued: 4 July 2024

Responsible officer: Finance Manager

INTRODUCTION

The Peak District National Park Authority (PDNPA) introduced a new cloud based finance system; iplicit, on 1 October 2023. This new system records all the financial activity of the PDNPA. It is used to prepare the annual accounts and various financial returns required by the Government.

Weekly bank reconciliations, accurate use of journals and appropriate use of suspense accounts are an important part of the financial internal control framework. A new bank reconciliation module is currenty being embedded within the new system, and the authority has introduced revised procedures to cover these areas.

OBJECTIVES AND SCOPE

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

- Bank reconciliations are performed on a regular basis and authorised appropriately
- Journals are accurately recorded and are appropriately authorised
- Access controls are appropriately allocated, reviewed and maintained
- Assurance is gained that backup retentions for the system are working as intended

At the time of the audit the opening balances for the new system had not been uploaded to iplicit due to the external audit for 2022/23 not yet being completed. Consequently, this work did not review the new systems opening balance sheet. We have confirmed that the balances have subsequently been uploaded.

KEY FINDINGS

The previous finance system, Exchequer did not have bank reconciliation functionality; however, we confirmed that weekly spreadsheets were being used to manually reconcile accounts. Upon review of these reconciliations, we confirmed that the process was robust and had been performed on a monthly basis. The new iplicit system has a bank reconciliation module which we found provided a clear audit log to demonstrate both regularity of reconciliations and appropriate authorisations in each instance. The weekly spreadsheets that were in use previously are still maintained to assist with monitoring income streams, but they no longer form part of the reconciliation process each month.

The Exchequer system did not require any authorisation or approval for journals, although we found that journal sheets were completed, and these had been retained and were available for examination. The iplicit system has a clear audit trail recording the creator and authoriser for all journals. We found that all journals sampled were appropriately authorised and recorded accurately.

Access to Exchequer and iplicit is managed by the finance team. Arrangements for new starters, leavers and volunteers were reviewed and it was confirmed that access is appropriately maintained. The review of all volunteer access is undertaken every 6 months, and the accounts are disabled for those users that have not accessed the expenses system within that timeframe. One large account cleanse has already been carried out on the new system. There are currently 5 members of finance staff who are admin users for iplicit, and they are able to create new user accounts and amend access rights.

A contract is in place between Azure and the National Park Authority, which outlines the services expected which includes a process for back-ups. However, there is no mention in the contract that Azure will provide regular assurance of this to the National Park Authority, and we have established that no evidence has been provided to date. Neither has the National Park Authority asked for any assurances over this same period. This matter was highlighted during the audit, and a one-off request for assurance was then made by the National Park Authority which Azure responded to by providing a log of back-up data. A further request for regular back-up information has since been submitted and the National Park Authority is now awaiting a formal response from Azure.

OVERALL CONCLUSIONS

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.

1 No confirmation of back-ups is received by the National Park Authority

Moderate

Control weakness

There is no monitoring or review of the back-up process as the supplier does not provide any information to the National Park Authority to confirm that back-ups have been taken or that any tests of the back-up data have been carried out.

What is the risk?

Back-ups are not taken and data is lost.

Findings

During the audit, we established that current contract requirements do not stipulate that Azure routinely provides any back-up related information to the National Park Authority for assurance purposes, nor has the National Park Authority previously asked for any confirmation that back-ups are being carried out or that data has been backed up accurately. A one-off request was then made to Azure by the National Park Authority on 4th March 2024 and a log containing back-up data was provided which demonstrated that Azure SQL Database automatically creates full database back-ups weekly, differential database back-ups every 12 hours, and transaction log back-ups every 5-10 minutes. The back-ups are stored for at least 7 days for all service tiers. An enhancement request was also submitted to Azure on 4th March 2024 to request regular visability of the back-up services being provided to the National Park Authority and a follow up request was also made on 7th May 2024 and the National Park Authority is now waiting on a formal response although Azure has confirmed that the request has been received.

Agreed action

Implementation and review of backup reports, expected imminently from service provider. If any delay in the report being built we will request directly in the Interim. Quarterly checks on robustness of backup reports to be reviewed and on a quarterly basis from Q3. Evidence will be retained and available for inspection by both Internal & External audit.

Responsible officer: Finance Manager **Timescale**: 31 December 2024

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 four grades of opinion, as set out below.

Opinion	Assessment of internal control
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.

Finding ratings

Critical	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Significant	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Moderate	The system objectives are not exposed to significant risk, but the issue merits attention by management.
Opportunity	There is an opportunity for improvement in efficiency or outcomes but the system objectives are not exposed to risk.