Report No. 16/23

Audit & Corporate Services Review Committee

REPORT OF THE INTERNAL AUDITOR

SUBJECT: INTERNAL AUDIT REPORT 2022/23

The report presents the remaining reports in respect of ICT review of Disaster Recovery and the final Annual Report 2022/23.

The Authority acknowledges the findings in the report and will respond to it recommendations accordingly.

Recommendation: Members are asked to NOTE and COMMENT on this report

(For further information, please contact Richard Griffiths, extension 4815 richardg@pembrokeshirecoast.org.uk)

ICT Audit

FINAL

Pembrokeshire Coast National Park Authority

ICT Review of Disaster Recovery

2022/23

June 2023

Executive Summary

OVERALL ASSESSMENT

ASSURANCE OVER KEY STRATEGIC RISK / OBJECTIVE

No strategic risks identified on the Risk Register.

KEY STRATEGIC FINDINGS

- **A Group is not in place to oversee Disaster Recovery (DR) and Business Continuity (BC) related matters.**
- **A published Business Continuity Plan (BCP) and a DR plan is not in place. The current plans require updating following the structural changes the organisation is experiencing.**
- **No BC and DR testing has been performed recently.**
- **Staff training is currently not provided as the BCP and DR plans need updating.**

GOOD PRACTICE IDENTIFIED

- **Regular backups are performed and checked by the IT Network Officer.**

SCOPE

The review considered the extent to which the organisation has put into place arrangements which provides reasonable but not absolute assurance that the impact on the organisation of any major incident will be minimised. The scope of the review did not include providing assurance that the actual testing of hardware/software etc has been carried out effectively.

ACTION POINTS

Urgent	Important	Routine	Operational
3	5	0	0

Assurance - Key Findings and Management Action Plan (MAP)

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
1	Directed	The IT Manager was responsible for overseeing Disaster Recovery (DR) and Business Continuity (BC) related concerns. This responsibility has recently been handed over to one individual - a newly appointed Head of Decarbonisation. A Group is currently not in place.	A Group be put in place to oversee DR and BC.	1	*Agreed.*	*31/12/23*	*Chief Executive and Head of Decarbonisation*

PRIORITY GRADINGS

1	URGENT	Fundamental control issue on which action should be taken immediately.
2	IMPORTANT	Control issue on which action should be taken at the earliest opportunity.
3	ROUTINE	Control issue on which action should be taken.

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
2	Directed	Originally raised as a finding in a previous review (2019/20), a published organisational BCP is still not in place. Pembrokeshire Coast National Park Authority (PCNPA) is currently going through a complete change in staffing structure. The job descriptions are to be revised and where each staff members will be located. The BCP will then need to be updated according to the new structure. The plan is reviewed on ad-hoc basis. The IT Network Officer and Head of Decarbonisation are responsible for reviewing the BCP and IT DR Plan. There are no departmental DR and BC policies in place. This was reviewed a few years ago, but as there has been re-organisation and formation of new departments, contingency arrangements are likely to be out of date. An up-to-date BCP distribution list is not in place as there has been numerous changes since 2015 when it was last updated. Many key staff members in the distribution list are no longer with the organisation.	The BCP be re-written to ensure that it reflects the current processes required to ensure that the organisation can continue operationally in recovering from a disaster, mishap or other event. Additionally, once the BCP has been agreed all nominated personnel be made aware of their responsibilities and trained accordingly. BCP hard copies to be made available once the BCP has been re-written and finalised. Individual policies per department be put in place if not already. If there are contingency arrangements, these to be reviewed and updated. The policies to cover scenarios such as IT outage (reverting to paper), staff sickness (i.e covid). An up-to-date distribution list be put in place so the BCP can be distributed to the right personnel when completed.	1	*Agreed.*	*31/12/23*	*Chief Executive and Head of Decarbonisation*

PRIORITY GRADINGS

1	URGENT	Fundamental control issue on which action should be taken immediately.
2	IMPORTANT	Control issue on which action should be taken at the earliest opportunity.
3	ROUTINE	Control issue on which action should be taken.

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
4	Directed	The current DR plan is in draft format since 2015. The revised DR Plan drafted but awaiting full implementation of Office 365 before adopting.	A DR policy be put in place which is detailed for the IT Team only as it will contain sensitive information such as IP addresses to be able to restore the systems. The DR plan be updated following the new structural changes to ensure organisation can recover from a disaster as quickly as possible.	1	*Agreed.*	*31/12/23*	*Chief Executive and Head of Decarbonisation*
3	Directed	There were no BC tests carried out recently. It was noted that during the covid pandemic BC arrangements were "tested" in a live scenario and reported to have been successful in ensuring no operational disruption.	The plan be tested on an annual basis and updated accordingly.	2	*Agreed. Once BCP is in place with we will test the plan accordingly*	*31/3/24*	*Head of Decarbonisation*
5	Directed	The DR Plan has not been tested as it is a historic document and does not meet the current requirements. The plan needs updating according to the new structure and BCP. It was not feasible to perform full testing due to the limitation of simulating a disaster situation. Limited testing had been performed in the past. PCNPA has moved to Microsoft 365 and will evaluate how testing is to be performed differently.	Regular testing be performed once the DR Plan has been updated.	2	*Agreed. Once BCP is in place with we will test the plan accordingly*	*31/3/24*	*Head of Decarbonisation*

PRIORITY GRADINGS

1	**URGENT**	Fundamental control issue on which action should be taken immediately.
2	**IMPORTANT**	Control issue on which action should be taken at the earliest opportunity.
3	**ROUTINE**	Control issue on which action should be taken.

Rec.	Risk Area	Finding	Recommendation	Priority	Management Comments	Implementation Timetable (dd/mm/yy)	Responsible Officer (Job Title)
6	Directed	Staff are not provided BC or DR training as both BCP and DR plans have not been formalised. The training is planned to be provided on ad-hoc basis once the plans have been finalised.	The staff be provided regular training once the plans have been formalised.	2	*Agreed once Plan(s) completed.*	*31/03/24*	*Management Team led by the Head of Decarbonisation*
7	Directed	PCPNA keeps a limited amount of backups and backups are retained for a limited period of time. Backups are stored on site and 365 tenant backups are made to a third party. Due to the unavailability of the IT Network Officer, it has not been confirmed if PCNPA has a contract is in place with the third party. Veeam Backup and Replication Version 11 is used to create onsite backups. Offsite tape backups are also retained which are planned to be moved to cloud services.	To confirm, if there is a contract in place with the third party responsible for backups and a copy of the contract to be provided.	2	*Agreed, we will confirm that contract is in place.*	*30/09/23*	*Head of Decarbonisation*
8	Directed	The offsite backups are secured in terms of storage. These are stored at an employees' house in a filing cabinet storage.	Backups be stored at the organisation's premises in a separate fire zone, until they can be retained on cloud services.	2	*We will explore other arrangements for backups off-site.*	*31/03/24*	*Head of Decarbonisation*

PRIORITY GRADINGS

1	URGENT	Fundamental control issue on which action should be taken immediately.
2	IMPORTANT	Control issue on which action should be taken at the earliest opportunity.
3	ROUTINE	Control issue on which action should be taken.

Operational - Effectiveness Matter (OEM) Action Plan

Ref	Risk Area	Finding	Suggested Action	Management Comments
No Operational Effectiveness Matters identified during the review.				

ADVISORY NOTE

Operational Effectiveness Matters need to be considered as part of management review of procedures.

Findings

Directed Risk:

Failure to properly direct the service to ensure compliance with the requirements of the organisation.

Ref	Expected Key Risk Mitigation		Effectiveness of arrangements	Cross Reference to MAP	Cross Reference to OEM
GF	**Governance Framework**	There is a documented process instruction which accords with the relevant regulatory guidance, Financial Instructions and Scheme of Delegation.	Not in place	1, & 2	-
RM	**Risk Mitigation**	The documented process aligns with the mitigating arrangements set out in the corporate risk register.	In place	-	-
C	**Compliance**	Compliance with statutory, regulatory and policy requirements is demonstrated, with action taken in cases of identified non-compliance.	Not in place	3, 4, 5, 6, 7, & 8	-

Other Findings
A central emergency contact list is not kept behind the reception. Most departments have their own lists for their specific areas.
TIAA did a review of the risk register, and the finding was it was too detailed, a recommendation was made to streamline. The BC/DR risks are on the risk register but not on the main critical list.
The backups are routinely checked. The IT Network Officer is emailed when the backup jobs are completed.

Delivery Risk:

Failure to deliver the service in an effective manner which meets the requirements of the organisation.

Ref	Expected Key Risk Mitigation		Effectiveness of arrangements	Cross Reference to MAP	Cross Reference to OEM
PM	Performance Monitoring	There are agreed KPIs for the process which align with the business plan requirements and are independently monitored, with corrective action taken in a timely manner.	Not in place	-	-
S	Sustainability	The impact on the organisation's sustainability agenda has been considered.	Out of scope	-	-
R	Resilience	Good practice to respond to business interruption events and to enhance the economic, effective and efficient delivery is adopted.	In place	-	-

Other Findings
BC and DR are not applicable to the sustainability agenda.

EXPLANATORY INFORMATION

Appendix A

Scope and Limitations of the Review

1. The definition of the type of review, the limitations and the responsibilities of management in regard to this review are set out in the Annual Plan. As set out in the Audit Charter, substantive testing is only carried out where this has been agreed with management and unless explicitly shown in the scope no such work has been performed.

Disclaimer

2. The matters raised in this report are only those that came to the attention of the auditor during the course of the review, and are not necessarily a comprehensive statement of all the weaknesses that exist or all the improvements that might be made. This report has been prepared solely for management's use and must not be recited or referred to in whole or in part to third parties without our prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose. TIAA neither owes nor accepts any duty of care to any other party who may receive this report and specifically disclaims any liability for loss, damage or expense of whatsoever nature, which is caused by their reliance on our report.

Effectiveness of arrangements

3. The definitions of the effectiveness of arrangements are set out below. These are based solely upon the audit work performed, assume business as usual, and do not necessarily cover management override or exceptional circumstances.

In place	The control arrangements in place mitigate the risk from arising.
Partially in place	The control arrangements in place only partially mitigate the risk from arising.
Not in place	The control arrangements in place do not effectively mitigate the risk from arising.

Assurance Assessment

4. The definitions of the assurance assessments are:

Substantial Assurance	There is a robust system of internal controls operating effectively to ensure that risks are managed and process objectives achieved.
Reasonable Assurance	The system of internal controls is generally adequate and operating effectively but some improvements are required to ensure that risks are managed and process objectives achieved.
Limited Assurance	The system of internal controls is generally inadequate or not operating effectively and significant improvements are required to ensure that risks are managed and process objectives achieved.
No Assurance	There is a fundamental breakdown or absence of core internal controls requiring immediate action.

Acknowledgement

5. We would like to thank staff for their co-operation and assistance during the course of our work.

Release of Report

6. The table below sets out the history of this report.

Stage	Issued	Response Received
Audit Planning Memorandum:	2nd February 2023	27th March 2023
Draft Report:	8th June 2023	8th June 2023
Final Report:	9th June 2023	

AUDIT PLANNING MEMORANDUM

Appendix B

Client:	Pembrokeshire Coast National Park Authority		
Review:	ICT Disaster Recovery		
Type of Review:	Assurance	**Audit Lead:**	Iqra Bakhtiyaar

Outline scope (per Annual Plan):	The review considers the extent to which the organisation has put into place arrangements which provides reasonable but not absolute assurance that the impact on the organisation of any major incident will be minimised. The scope of the review does not include providing assurance that the actual testing of hardware/software etc has been carried out effectively.	
Detailed scope will consider:	Directed Governance Framework: There is a documented process instruction which accords with the relevant regulatory guidance, Financial Instructions and Scheme of Delegation. Risk Mitigation: The documented process aligns with the mitigating arrangements set out in the corporate risk register. Compliance: Compliance with statutory, regulatory and policy requirements is demonstrated, with action taken in cases of identified non-compliance.	Delivery Performance monitoring: There are agreed KPIs for the process which align with the business plan requirements and are independently monitored, with corrective action taken in a timely manner. Sustainability: The impact on the organisation's sustainability agenda has been considered. Resilience: Good practice to respond to business interruption events and to enhance the economic, effective and efficient delivery is adopted.
Requested additions to scope:	None	
Exclusions from scope:	The scope of the review does not include providing assurance that the actual testing of hardware/software etc has been carried out effectively.	

Planned Start Date:	27/03/2023	**Exit Meeting Date:**	05/06/2023	**Exit Meeting to be held with:**	IT Network Officer

SELF ASSESSMENT RESPONSE

Matters over the previous 12 months relating to activity to be reviewed	**Y/N (if Y then please provide brief details separately)**
Has there been any reduction in the effectiveness of the internal controls due to staff absences through sickness and/or vacancies etc?	N
Have there been any breakdowns in the internal controls resulting in disciplinary action or similar?	N
Have there been any significant changes to the process?	Y – staff structure changes
Are there any particular matters/periods of time you would like the review to consider?	N

Internal Audit

FINAL

Pembrokeshire Coast National Park Authority

Internal Audit Annual Report

2022/23

June 2023

Internal Audit Annual Report

Introduction

This is the 2022/23 Annual Report by TIAA on the internal control environment at Pembrokeshire Coast National Park Authority. The annual internal audit report summarises the outcomes of the reviews we have carried out on the Pembrokeshire Coast National Park Authority's framework of governance, risk management and control.

Our approach is based on the International Standards for the Professional Practice of Internal Auditing which have been developed by the Institute of Internal Auditors (IIA) and incorporate the Public Sector Internal Audit Standards (PSIAS). In 2022, TIAA commissioned an External Quality Assessment (EQA) of its internal audit service. The independent EQA assessor was able to conclude that TIAA 'generally conforms to the requirements of the Public Sector Internal Audit Standards and the mandatory elements of the Institute of Internal Auditors (IIA) International Professional Practices Framework (IPPF).' 'Generally conforms' is the highest rating that can be achieved using the IIA's EQA assessment model. Ongoing quality assurance work was carried out throughout the year and we continue to comply with ISO 9001:2015 standards.

HEAD OF INTERNAL AUDIT'S ANNUAL OPINION

TIAA is satisfied that, for the areas reviewed during the year, Pembrokeshire Coast National Park Authority has reasonable and effective risk management, control and governance processes in place. One area, ICT Disaster Recovery, was reviewed by internal audit where it was assessed that the effectiveness of some of the internal control arrangements provided 'limited assurance'. Recommendations were made to further strengthen the control environment in this area and management have accepted the recommendations and provided appropriate responses.

This opinion is based solely on the matters that came to the attention of TIAA during the course of the internal audit reviews carried out during the year and is not an opinion on all elements of the risk management, control and governance processes or the ongoing financial viability or your ability to meet financial obligations which must be obtained by Pembrokeshire Coast National Park Authority from its various sources of assurance.

Internal Audit Planned Coverage and Output

The 2022/23 Annual Audit Plan approved by the Audit and Corporate Services Review Committee was for 25 days of internal audit coverage in the year.

During the year there was one change to the Audit Plan and this change was approved by the Audit and Corporate Services Review Committee. The planned review of the Board Assurance Framework has been deferred to 2023/24.

The planned work that has been carried out against the plan and the status of work not completed is set out at Annex A.

No extra work was carried out which was in addition to that set out in the Annual Audit Plan.

Assurance

TIAA carried out seven reviews, six of which were designed to ascertain the extent to which the internal controls in the system are adequate to ensure that activities and procedures are operating to achieve Pembrokeshire Coast National Park Authority's objectives. For each assurance review an assessment of the combined effectiveness of the controls in mitigating the key control risks was provided. Details of these are provided in Annex A and a summary is set out below.

Assurance Assessments	Number of Reviews	Previous Year
Substantial Assurance	3	2
Reasonable Assurance	2	4
Limited Assurance	1	0
No Assurance	0	0

The areas on which the assurance assessments have been provided can only provide reasonable and not absolute assurance against misstatement or loss and their effectiveness is reduced if the internal audit recommendations made during the year have not been fully implemented.

We made the following total number of recommendations on our audit work carried out in 2022/23. The numbers in brackets relate to 2021/22 recommendations.

Urgent	Important	Routine
3 (0)	11 (10)	13 (14)

Audit Summary

Control weaknesses: There was one area reviewed by internal audit (ICT Disaster Recovery) where it was assessed that the effectiveness of some of the internal control arrangements provided 'limited assurance.' Recommendations were made to further strengthen the control environment in these areas and the management have accepted the recommendations and completed appropriate responses.

Recommendations Made: We have analysed our findings/recommendations by risk area and these are summarised below.

Risk Area	Urgent	Important	Routine
Directed			
Governance Framework	2 (0)	1 (3)	5 (4)
Risk Mitigation	0 (0)	0 (0)	0 (0)
Compliance	1 (0)	8 (7)	7 (7)
Delivery			
Performance Monitoring	0 (0)	1 (0)	1 (2)
Sustainability	0 (0)	0 (0)	0 (0)
Resilience	0 (0)	1 (0)	0 (1)

[1] This excludes the Board Assurance Framework review which did not take place at Management's request.

Operational Effectiveness Opportunities: One of the roles of internal audit is to add value and during the financial year we provided advice on opportunities to enhance the operational effectiveness of the areas reviewed and the number of these opportunities is summarised below.

Operational
2 (6)

Independence and Objectivity of Internal Audit

There were no limitations or restrictions placed on the internal audit service which impaired either the independence or objectivity of the service provided.

Performance and Quality Assurance

The following Performance Targets were used to measure the performance of internal audit in delivering the Annual Plan.

Performance Measure	Target	Attained
Completion of Planned Audits	100%	100%[1]
Audits Completed in Time Allocation	100%	100%
Final report issued within 10 working days of receipt of responses	95%	100%
Compliance with IIA Internal Audit Standards	100%	100%

Release of Report

The table below sets out the history of this Annual Report.

Date Indicative Report issued:	11th May 2023
Final Report issued:	22nd June 2023

Annexes

Annex A

Actual against planned Internal Audit Work 2022/23

System	Type	Planned Days	Actual Days	Assurance Assessment	Comments
Board Assurance Framework - Advisory	Advisory	2	0	N/A	Deferred to 2023/24 at the request of Management
ICT Disaster Recovery	Assurance	3	3	Limited	Final Report Issued
Safeguarding	Assurance	3	3	Substantial	Final Report Issued
Visitor Centres & Cafes - Castell Henllys	Compliance	2	2	Reasonable	Final Report Issued
Performance Management	Assurance	3	3	Reasonable	Final Report Issued
Payroll and Expenses	Assurance	3	3	Substantial	Final Report Issued
Conservation Management Schemes	Assurance	3	3	Substantial	Final Report Issued
Follow-up	Follow up	1	1	N/A	Final Report Issued
Annual Planning	Management	1	1		Final Plan Issued
Annual Report	Planning/Reporting	1	1		Final Report Issued
Audit Management	Planning/Reporting	3	3		
	Total Days	**25**	**23**		