Appendix 2

IT BUSINESS CONTINUITY AND DISASTER RECOVERY

PEAK DISTRICT NATIONAL PARK AUTHORITY

INTERNAL AUDIT REPORT

	Critical	Significant	Moderate	Opportunity
Findings	0	1	2	0
Overall audit opinion	**Substantial assurance**			

Status: Final

Date Issued: 16 September 2025

Responsible Officer: Head of Resources

Veritau

INTRODUCTION

IT business continuity is the process of designing, building, and maintaining a framework that ensures an organisation can continue operating during, and recover quickly from, disruptive events such as cyberattacks or loss of IT services. Closely linked, IT disaster recovery focuses specifically on restoring technology systems and services after such an event. Effective plans in these areas should set out a structured and timely response, enabling disruption to be reduced to a predetermined and acceptable level.

The Peak District National Park Authority (the authority) outsources the majority of its IT services to third-party providers. Core functions such as infrastructure hosting, firewall protection, and secondary data centre provision are outsourced to Iomart. In this context, robust backup arrangements are essential to ensure systems can be restored within agreed timescales and with minimal data loss, limiting the impact of any incident. The authority is currently assessing options for a new backup solution as part of ongoing resilience improvements.

Nevertheless, the authority maintains responsibility for its IT business continuity and disaster recovery plan. To be effective these arrangements must not only be documented but also regularly tested. Lessons learnt from tests should be captured and embedded into updated plans, ensuring that resilience evolves alongside technology changes, supplier arrangements, and emerging threats.

OBJECTIVES AND SCOPE

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

- Robust plans and preparations are in place to ensure recovery of systems and data within the authority's recovery time objective following an incident.
- Disaster recovery roles and responsibilities are clearly documented, kept up to date, and include assigned alternates.
- Backups are taken in line with recovery objectives, stored securely, and tested successfully, with planned improvements assessed for effectiveness.
- The IT business continuity plan is reviewed and tested periodically, with lessons learned incorporated into updates.

KEY FINDINGS

The authority has a documented and up-to-date business continuity plan (BC plan), with an ICT disaster recovery plan (DR plan) included at appendix two. The plan is reviewed and updated regularly, and it incorporates many of the core features of good practice. The plan is readily accessible to those with defined responsibilities and runbooks are being developed to provide IT staff with practical guidance for specific incident types, which should allow for more effective recovery.

However, the DR plan is not underpinned by a comprehensive business impact assessment (BIA) aligned to recognised best practice principles. It also does not set out recovery time objectives, recovery point objectives and maximum tolerable periods of disruption (RTOs, RPOs and MTPDs).

Additionally, the scope of incident scenario planning within the DR plan is limited. At present, it does not cover a full range of scenarios as recommended by the National Cyber Security Centre (NCSC) guidance, although progress is being made through the development of incident-specific runbooks, with ransomware already completed and others in development. In addition, the NCSC advises that DR plans should set out clear processes for reporting incidents externally, including to the Information Commissioner's Office (ICO). The authority's DR plan does not currently define a reporting route.

The BC plan defines emergency response roles, but the DR plan does not assign roles or responsibilities for IT-related incidents. Formal training on DR has not yet taken place, although a programme of scenario-based exercises is planned, beginning with a malware exercise-in-a-box in October 2025. This approach will also broaden the scope of DR testing beyond bubble testing and provides increasing assurance that the DR plan will be actively tested.

The authority has robust backup arrangements, supported by Iomart. Backups are completed in line with the recognised GFS backup strategy and stored securely within UK-based cloud locations. Files are backed up daily, with evidence provided by Iomart and reviewed by IT services. Ad-hoc file restores are carried out regularly, providing practical assurance that data can be recovered when required. In addition, previous bubble testing has confirmed the ability to recover from a failover site.

While there is currently no formal backup testing schedule, compensating controls are in place through monitoring, ad-hoc restores, and the last bubble test. Planned annual bubble testing from 2026, as part of the move to a new IaaS solution, will strengthen assurance and align more closely with best practice. The new Cohesity Backup-as-a-Service platform is expected to deliver further resilience benefits, including more frequent recovery points for critical systems. Governance and approval routes for implementation are in place, with rollout planned for early 2026.

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 Runbooks and training — Significant

Control weakness

Only one incident-specific runbook (malware) has been developed to date, and no formal training has yet been provided to IT staff on its use.

What is the risk?

The authority is not prepared for IT incidents, increasing the time taken to respond and recover data and systems.

Findings

NCSC[1] guidance emphasises the importance of documenting incident-specific response procedures within the Disaster Recovery (DR) plan or through runbooks. These should set out roles, responsibilities, and step-by-step actions to be followed in different scenarios, supported by training and exercising so that staff can respond effectively during an incident.

At present, the authority's DR plan remains high level and does not provide the expected range of incident-specific responses. Only one runbook has been developed, covering malware, which aligns with NCSC best practice principles. Further runbooks are planned, with several expected to be completed before 2026, but current coverage is limited.

Furthermore, IT staff have not yet received formal training on disaster recovery or on the use of the malware runbook. A programme of scenario-based training is planned, beginning with an exercise-in-a-box tabletop exercise on malware scheduled for October 2025, with further exercises to follow as additional runbooks are developed. While progress is being made, the current arrangements do not fully align with NCSC best practice. Until this work is completed, it remains unclear whether the authority could respond effectively and consistently to different disaster recovery scenarios.

Agreed action

A wider range of incident specific runbooks will be developed to cover a range of DR scenarios. Following this a programme of training through exercising will be developed to ensure staff are familiar with procedures.

Responsible officer: IT Manager **Timescale:** 31 March 2026

[1] https://www.ncsc.gov.uk/collection/cyber-assessment-framework/caf-objective-d/principle-d1-response-and-recovery-planning

2 BIAs and recovery objectives

Moderate

Control weakness

A comprehensive IT BIA has not been completed and the DR plan does not set out RTOs, RPOs or MTPDs.

What is the risk?

Recovery priorities do not reflect business requirements or risk appetite. This may result in critical systems not being restored within acceptable timescales, leading to extended service disruption.

Findings

ISO 22301 (Section 8.2.2) and the Government's Business Continuity Management Toolkit[2] emphasise that DR priorities and objectives should be underpinned by BIAs. These identify critical systems and services, evaluate the impacts of disruption over time, and define recovery objectives such as RTOs, RPOs, and MTPDs.

At present, a comprehensive IT services BIA has not been completed. Some BIA data has been captured within Data Protection Impact Assessments, but the BIA element does not align with best practice. It does not identify critical systems, assess disruption impacts, or set out recovery objectives and resource requirements. This limits its value in informing recovery planning, as reflected by the absence of recovery objectives in the DR plan.

The DR plan does include a priority order for the restoration of services, which appears mostly logical. However, this sequence is dictated primarily by technical dependencies and licensing limitations, rather than by the outcomes of a BIA. As a result, it is unclear whether the order reflects organisational priorities or risk appetite. For example, if a BIA were completed, the current prioritisation of restoring the website ahead of remote connectivity may have been reconsidered.

Agreed action

A BIA will be completed to identify critical systems and assess the impact of disruption over time to determine recovery objectives for inclusion in the DR plan.

Responsible officer: IT Manager **Timescale:** 31 March 2026

[2] https://assets.publishing.service.gov.uk/media/5a7b283de5274a34770e9d01/Business_Continuity_Managment_Toolkit.pdf

3 Roles and responsibilities — Moderate

Control weakness

The DR plan does not assign defined roles and responsibilities for IT incidents, nor does it set out clear responsibilities and a process for external reporting requirements such as notifying the ICO or NCSC of an incident.

What is the risk?

Incident response could be delayed or inconsistent, and regulatory reporting requirements may not be met. This could result in extended disruption and reputational damage.

Findings

ISO 22301 (section 8.4.4) states that "business continuity plans shall contain defined roles and responsibilities for people and teams having authority during and following an incident." NCSC guidance also emphasises that incident response plans should identify who is responsible for decision-making, technical actions, communications, and external notifications. These principles ensure that when an incident occurs, responsibilities are clear and actionable.

While the BC plan defines an Emergency Response Team, the Incident Response Team is not documented, and the DR plan contains no specific IT roles. This was intended to preserve flexibility but creates uncertainty over accountability in practice. Runbooks provide some clarity, for example the malware runbook defines IT responsibilities by role, and further runbooks are in development. These are positive steps, but runbooks are not a substitute for core role definitions within the DR plan. NCSC best practice is that at least a core IT incident response team should be documented in the plan.

The DR plan also omits external reporting routes, including the statutory requirement to notify the ICO where thresholds are met and recommended engagement with the NCSC in the event of serious cyber incidents. Incorporating this responsibility and processes into the plan would strengthen compliance and ensure consistent escalation.

Agreed action

The DR plan will be updated to define a core IT incident response team by role and include clear external reporting routes and responsibilities for notifiable incidents (i.e. ICO reporting).

Responsible officer: IT Manager **Timescale:** 31 March 2026

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	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.

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.