Appendix 1

IT Access Controls and User Awareness

Peak District National Park Authority

Internal Audit Report 2021/22

Business Unit: Information and Performance Management
Responsible Officer: Head of Information and Performance Management
Service Manager: IT Manager
Date Issued: 7 January 2022
Status: Final
Reference: 69180/003

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

Summary and Overall Conclusions

Introduction

Organisations such as the Peak District National Park Authority (PDNPA) are reliant on technology to store and access data. Therefore it is essential that there are comprehensive security measures in place that help ensure data, systems and assets are protected from damage, unauthorised access, loss and misuse.

The PDNPA utilise third party systems to support the authority's services. These systems are used for a number of purposes such as administering cycle hire and allowing residents to submit planning applications electronically. If the Authority do not have controls in place to maintain the security of customer data then they risk breaching GDPR regulations and suffering reputational damage. One important area of keeping applications secure is ensuring access to the systems is limited to authorised individuals only.

The most prolific method of distributing malicious software or allowing unauthorised individuals to gain access to an organisations network and data is via phishing emails. Phishing is where an attacker masquerades as a trusted entity to convince a victim into opening an email. Phishing attacks are becoming more sophisticated to get around email filters and appear like a genuine email. The National Cyber Security Centre highlights the importance of staff cyber security awareness training in reducing the likelihood and impact of a successful phishing attack.

Objectives and Scope of the Audit

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

- Access controls were appropriately authorised and monitored in third party applications.
- Suitable training and guidance was provided to staff to raise cyber security awareness.

Key Findings

The Authority has appropriate access controls in place for its third party applications and access to these applications was appropriately authorised and monitored. We saw that there are clear processes for adding and removing users from third party applications. There is clear governance in place for managing applications and responsibility for adding and removing users had been delegated to a primary and secondary administrator for each application. System administrators monitor user access for the systems. In addition to this, the Web Manager carries out regular reviews on the management of applications which checks that monitoring is taking place. We reviewed the list of users with administrative or editorial access to applications and saw that access levels were linked to job roles and all seemed reasonable. There were also appropriate password requirements in place for each of the applications.

We found there were a number of measures in place to raise awareness of cyber security risks in the Authority. The Information Management Policies Framework covers acceptable usage of IT and instructs users on appropriate action to take if they have any cyber security related concerns. One area of improvement that could be made to the policy is to add disciplinary actions if the policy has not been followed. ISO 27002 control objectives recommend that the information security policy should contain disciplinary procedures for instances where the policy is breached. This would act as a deterrent against breaching the policy and would also make it easier for the Authority to take appropriate action in the event of ICT misuse. We saw that the policy was up to date and had been reviewed regularly. Users are required to complete an online form to confirm they have read and understood the policy before being granted access to PDNPA systems.

The Authority have also rolled out a phishing email training exercise whereby staff were sent fabricated phishing emails and staff responses to receiving the emails were monitored. The Authority recorded whether staff opened, clicked, or opened and clicked on the emails. A total of 310 staff received between 2 and 6 fake phishing emails with 109 staff clicking on at least one email. Staff that clicked on one of these fake phishing emails were then directed towards training on phishing emails based on their response to the fabricated phishing emails, for example staff identified as ‘repeat offenders’ were given additional training. There is a review planned for January 2022 to ascertain which staff have training outstanding and to take action to remedy this. In addition to the phishing training, staff in the IT department have taken further training on Data Security via the ELMS system.

Communication of the cyber security risks facing the Authority is good. The quarterly Corporate Authority Performance Report includes KPIs for data security and there is also an Information Management Service risk register covering ransomware, hacks, DDoS, and internal threats.

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.

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.

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.