Veritau
Assurance Services for the Public Sector

IT Systems Controls

Peak District National Park Authority

Internal Audit Report 2017/18

Business Unit: ICT
Responsible Officer: Director of Corporate Services
Service Manager: Head of Information Management
Date Issued: 23 March 2018
Status: Final
Reference: 69180/002

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

PEAK DISTRICT NATIONAL PARK

Summary and Overall Conclusions

Introduction

Local Authorities are becoming ever more reliant on ICT. Councils are using data electronically because it is the most practical and effective way of working. There will likely be increased amounts of data stored within an Authorities network and a greater 'business need' to have network availability. All these factors mean there is a higher level of inherent risk around network security.

A lack of effective security controls within the Authority's network will increase the likelihood of data breaches and people having access to information they should not have. Also the risk that malicious software is used to corrupt the Authority's data has been increasing. Recent research from Barracuda Networks has revealed that 27% of UK local authorities have been affected by ransomware.

ICT services are currently provided by a third party (Server Choice) to Peak District National Park Authority (PDNPA). These services are agreed in a number of Service Level Agreements (SLAs).

Objectives and Scope of the Audit

The purpose of this audit was to provide assurance to management that IT systems, procedures and controls will ensure that:

- The performance of the ICT provider (Server Choice) is monitored to ensure standards set out in the contract are met.
- PDNPA comply with mandated requirements set out in the contract with Sever Choice.
- Access controls are in place to ensure only authorised individuals have access to the authority's data

Key Findings

We have found the authority have effective controls in place to protect the authority's data. Server Choice are meeting the requirements set out in the contract between the two organisations. The PDNPA ICT team have a procedure in place to monitor the performance of Server Choice in line with the contract.

The PDNPA ICT team have obtained assurance that data is secure within the 3rd party's data centre. The ICT team have also been proactive in ensuring data was not at risk when flaws to ICT hardware came to light. Server Choice is responsible for patching the authority's operating system. There is a procedure in place to ensure patches were updated and PDNPA has a record of all updates carried out. There is a suitable roll back procedure in place encase there is an issue with any of the patches.

Server Choice is responsible for completing regular backups of PDNPA data. Officers have confirmation of when backups have been taken. A full organisation wide system back up test has not been carried out. However individual components of the network have been successfully restored from back up.

The Information Management policy informs users of the acceptable use of ICT equipment. All staff are required to sign up to confirm they understand and will follow the policy. The policy is currently under review, following the implementation of a new Business Continuity plan and the introduction of GDPR in May 2018.

There is a procedure in place to ensure that the software licences are up-to-date. There is strong logical access controls in place to ensure that only authorised staff are provided with access.

ICT assets have antivirus software installed on the machines to safeguard against malware. The antivirus software on a small number of assets has not been updated with the latest version software, within one year. This is because the computers have not been connected to the network within this period.

All the assets are managed by the I.T team. Following the 2014/15 audit report it was agreed that IT will perform 6 monthly checks for assets that have reported as not connected to the network for a period of 3 months or more. It was also agreed that an inventory check would be carried out by a member of the finance team. These procedures have not occurred.

Overall Conclusions

The arrangements for managing risk were good with few weaknesses identified. An effective control environment is in operation, but there is scope for further improvement in the areas identified. Our overall opinion of the controls within the system at the time of the audit was that they provided Substantial Assurance.

1 Testing of Disaster Recovery Arrangements.

Issue/Control Weakness	Risk
The authority has not carried out a full disaster recovery test, since there has been a change in I.T infrastructure.	Issues may not be identified within the current disaster recovery arrangements. This may increase the time taken to restore the network following a network outage.

Findings

Since January 2017 Server Choice has been responsible for the restoration of systems following a network outage. In the contract between PDNPA and Server Choice it states 'DR testing is to take place on a 6 monthly basis initially, and upon agreement by the Customer, more infrequently (e.g. Annually or every two years).'

At the time of audit review (January 2018) PDNPA had not carried out any organisation wide tests of disaster recovery arrangements.

The I.T team have made an agreement with Server Choice to carry out a full system disaster recovery test in November 2018.The Authority have not carried out a full network disaster recovery test due to a high volume of work load. This is also partly due to the complication that if PDNPA was to carry out a test of the disaster recovery arrangements they would be charged extra from Oracle for duplicating licenses. Therefore the authority had to find a way of testing the disaster recovery provisions without including Oracle components.

The authority had requested Server Choice carry out tests of individual components of the network which had all been carried out successfully.

Agreed Action 1.1

As noted in this finding, several partial tests have been completed, and work has been progressed in order to disaster test as much of the overall infrastructure as is reasonable without incurring significant licencing costs (note: the licencing issue is accounted for in plans for a disaster and so the issue only applies to simulated scenarios).
As such, a more comprehensive test for the disaster recovery provisions can now be scheduled, and will therefore take place by the end of July 2018.

Priority	3
Responsible Officer	IT Support Officers (*2)
Timescale	31 July 2018

2 ICT Asset Management.

Issue/Control Weakness	Risk
There is no compensating control in place to verify that the authorities' asset management software is accurate. A small percentage of computers are not used on a regular basis and therefore do not have the latest antivirus updates applied.	Items, including those containing Authority data, may be lost.

Findings

I.T assets are purchased, monitored and disposed of by the I.T team. The assets location and current user information is logged on an asset management system. There is a small risk that members of the I.T team could dispose of the assets for their personal gain. Following the 2014/15 audit report the authority agreed for a member of the finance team to carry out a periodic independent sample check of ICT hardware invoices which is verified back to the IT inventory. There was no record of this check being carried out and the finance team did not have access to the ICT asset management system, at the time of testing. This is an important compensating control if the authority has machines that are not used for large periods of the year.

The authority has antivirus software loaded on to computers to prevent malicious software from corrupting data. We found out of 314 of the authority's computers, 10 of the computers antivirus software has not been updated in six months. There was a further 4 that had not been updated for more than one year. The laptop antivirus software automatically updates when the computer is connected to the network. Therefore the software is not updated frequently. There is a small risk the computers do not have adequate protection if they are switched on for the first time after being unused for large period of time. In the 2014/15 audit report it was agreed that IT will perform 6 monthly checks for assets that have reported as not connected to the network for a period of 3 months or more. There is no indication to show that this has occurred. This emphasise the importance of carrying out a stock check independent from the I.T team.

Agreed Action 2.1

A) The Finance team will ensure that an independent sample check of the IT inventory is undertaken annually

B) Not all computers operate on the PDNPA network. Many of the devices that are reporting as missing virus definitions or as having not connected in 6 months or a year are based at offices that are not on the PDNPA network, and so it is expected behaviour for these devices to show as not connecting for a long period of time. That said however, the virus definitions should still be updating, as the current antivirus

Priority	3
Responsible Officer	Part A – Finance Officers Part B – Head of Information Management
Timescale	Part A – Completed

software will update through any internet connection and is therefore independent of the PDNPA network.

To mitigate this, improved reporting will be created that will take into account:

- Data from Active Directory showing when a device last connected to the network
- Data from ESET showing when the virus definitions last updated
- Data from the Asset management system showing devices expected to be included in one of the two elements above as well as data showing when an IT support office last inspected that device.

This report will be reviewed on a 6 monthly basis and any unplanned cases of devices not connecting to the network, not having been inspected by an IT support officer and/or not having an up to date anti-virus definition will be investigated further by a member of the IT team.

To supplement this, as a part of the ongoing work to increase network access security, we will also investigate whether it is possible to deny network access to devices that have not received a virus definition update within a reasonable amount of time.

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.

PEAK DISTRICT NATIONAL PARK