Cairngorms National Park Authority

INTERNAL AUDIT REPORT

IT General Controls Review

June 2017

LEVEL OF ASSURANCE	
Design	Operational Effectiveness
Limited	Limited

BDO

CONTENTS

Appendices:

REPORT STATUS	
Auditors:	Andrew O'Donnell
Dates work performed:	April/May 2017
Draft report issued:	7 June 2017
Final report issued:	**18 August 2017**

DISTRIBUTION LIST	
David Cameron	Director of Corporate Services
Sandy Allan	IT Manager

Restrictions of use

The matters raised in this report are only those which came to our attention during the course of our audit and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. The report has been prepared solely for the management of the organisation and should not be quoted in whole or in part without our prior written consent. BDO LLP neither owes nor accepts any duty to any third party whether in contract or in tort and shall not be liable, in respect of any loss, damage or expense which is caused by their reliance on this report.

EXECUTIVE SUMMARY

LEVEL OF ASSURANCE (SEE APPENDIX II FOR DEFINITIONS)		
Design	🟠	System of internal controls is weakened with system objectives at risk of not being achieved.
Effectiveness	🟠	Non-compliance with key procedures and controls places the system objectives at risk.

SUMMARY OF RECOMMENDATIONS (SEE APPENDIX II)		
High	▲	
Medium	🟧	8
Low	🟢	3
Total number of recommendations: 11		

OVERVIEW

Background

Cairngorms National Park Authority (the Authority) is reliant on its ICT infrastructure and business systems to deliver services effectively to internal and external stakeholders. As part of the 2016-17 Internal Audit Plan, it was agreed with Internal Audit and Management that we would carry out an assessment of the general technology control environment by considering the adequacy of network security at both the logical and physical layers. We also assessed arrangements in place for the monitoring, maintenance and administration of the network and network devices. A core part of our review was to assess the level of resilience and redundancy built into the network by considering arrangements in place to ensure network availability, successful processing of data backups and ICT disaster recovery planning. We also reviewed the adequacy of service desk arrangements including incident, change and performance management.

Scope and Approach

The purpose of the review was to assess the general controls in place in relation to information technology. The review focussed on physical and logical access controls, system support arrangements, and program change controls.

Our review sought to gain assurance over whether:

- Network security policy and acceptable usage guidance had been developed and published;
- Powerful access to the network was controlled (to prevent the misuse of privileged administrator level accounts);
- There was effective user access and authorisation controls in place for staff and third parties, including the management of new starts, movers and leavers;

(Continued over)

EXECUTIVE SUMMARY

OVERVIEW

- Network password settings were in line with policy requirements and best practice recommendations;
- Remote access to the network was securely configured;
- Wireless access to the network was securely configured;
- Network devices have been built and deployed in a secure manner;
- There is regular security vulnerability scanning and network perimeter testing;
- Network devices have been patched in line with supplier recommendations;
- Firewalls and other security appliances have been deployed and their configuration is securely administered and maintained;
- There are physical and environmental security controls in place for data hosting facilities;
- There is network security monitoring and filtering including: anti-virus, mail scanning and internet content filtering;
- Network data back-ups are processed in an effective manner;
- Effective IT disaster recovery arrangements have been implemented; and
- Effective network security monitoring, logging and incident response procedures have been implemented.

Our approach was to conduct interviews to establish the controls in operation for each of our areas of audit work. We then sought documentary and system-based evidence that these controls were operating as designed as described. We evaluated these controls to identify whether they adequately address the risks. We sought to gain evidence of the satisfactory operation of the controls to verify the effectiveness of the control through use of a range of tools and techniques.

Good Practice

Areas of good practice identified during the review:

- An Information Security Policy, with defined security principles and roles and responsibilities, and an ICT policy with network acceptable usage guidance have been established as part of the data governance framework within the Authority;
- Domain administrator accounts which provide privileged access to the network resource/file system are effectively managed;
- Default Windows accounts such as ‘guest’ and ‘administrator’ have been hardened (i.e. publicly known default settings have been changed to prevent account misuse);
- There is effective management and control of third party network accounts;
- Requests for staff new starts and movers are handled in an effective manner;

(Continued over)

EXECUTIVE SUMMARY

OVERVIEW

- Network password and account lockout policy settings for user machines are securely configured;
- Remote access to the network is provisioned in a secure manner;
- Both corporate and guest wireless networks are logically separated and encrypted;
- There are adequate physical and environmental security controls in place for data hosting facilities;
- Anti-virus and mail scanning solutions have been deployed to protect the network; and
- There is adequate levels of security in place for mobile devices.

Key Findings

Key areas of improvement identified during the review:

- **Security awareness training** - network users have not been provided with an adequate level of network and data security awareness training;
- **Use of shared accounts** - IT staff are making use of shared accounts to administer the network. As a result, there is no unique accountability or attribution possible with respect to these accounts;
- **Network leavers** – we identified a number of exceptions where staff leaver accounts had not been disabled/removed from the network;
- **Patch testing** - there is currently no testing of Windows patches before these are deployed to the live environment;
- **Web content filtering** - current web content filtering settings could be further enhanced to minimise the level of security risk posed to the network;
- **Data backups** – there are currently no formal processes in place for the monitoring and testing of data backups;
- **Disaster recovery planning** - there is no IT disaster recovery (DR) plan in place to support the recovery of infrastructure and business systems following an IT disaster; and
- **End-point security** - staff are able to make use of unencrypted USB devices on the network and USB devices connecting to the network are not subject to security scanning.

(continued over)

EXECUTIVE SUMMARY

OVERVIEW

Conclusion

Based on the findings of this review, we have concluded that we can provide Limited assurance over the design and operation of IT general controls within the Authority. As well as identifying a number of areas of good practice we have also made a series of medium and low level priority recommendations for management attention and action. The more immediate priorities relate to the monitoring and testing of data backups as well as disaster recovery planning to ensure hardware and systems can be recovered in line with business requirements following an IT disaster. This is a key assurance area for the audit given the recent high-profile security incidents such as WannaDecryptor and the British Airways system failure. The risk in this area is further heightened given the growing trend of ransomware attacks. Effective data backups and disaster recovery planning would be essential in ensuring the continuity of business processes in these circumstances. Complementing this, we have also identified the need to raise the level of security awareness amongst users within the organisation. This is especially important now as improvements in enterprise level security have pushed threat actors to imaginatively, and often effectively, harness social engineering as a key component when launching their attacks.

EXECUTIVE SUMMARY

RISKS REVIEWED GIVING RISE TO NO FINDINGS OF A HIGH OR MEDIUM SIGNIFICANCE	
☑	Security incident monitoring and response procedures are ineffective.

EXECUTIVE SUMMARY

AREAS FOR IMPROVEMENT

Ref.	Sig.	Finding Summary	Recommendation
1	🟧	Our audit noted that network users have not been provided with and adequate level of computer security awareness training. Also, there is no training programme in place to ensure staff understand their responsibilities with respect to protecting and securing Authority data.	We recommend that all users are provided with computer security awareness training. This may take the form of group-based seminars or workshops and could be supplemented by on-line test-based learning.
2	🟧	Our audit noted that both IT organisations are making use of shared accounts to administer the network. As a result, there is no unique accountability or attribution possible with respect to these accounts.	We recommend that, where possible, use of shared use accounts on the network is minimised. We recommend that third party and partner organisations (i.e. LLTPA) are set up with their own uniquely named accounts. We recommend that the password for the default firewall administrator account is changed once unique accounts are created for LLTPA and Authority IT staff.
3	🟧	Our testing of network user accounts identified a number of exceptions where leaver accounts had not been disabled/removed from the network. We were advised that this may have resulted from slow processing of paperwork from line management or HR.	We recommend that network accounts for leavers are disabled as soon as the account owner leaves employment with the Authority. Controls should also ensure that accounts for temporary, agency or contract staff are disabled promptly when they are no longer required.
4	🟧	Our audit noted that there is currently no testing of Windows patches before these are deployed to the live environment.	We recommend that all patches are tested and deployed in a controlled phased manner across the server and desktop estate. We recommend that patches are first tested on a smaller group of non-business critical servers (or test servers that mirror the live environment) to assess whether these result in any adverse consequences to Authority systems before they are rolled out across the rest of the server estate.

All our findings and recommendations are set out in the following pages and include those of low significance which have not been summarised above.

EXECUTIVE SUMMARY

AREAS FOR IMPROVEMENT

Ref.	Sig.	Finding Summary	Recommendation
5	🟧	Our audit found that current web content filtering settings could be further enhanced to minimise the level of risk posed to the corporate network through general user access to the internet.	We recommend that current web content filtering settings are reviewed and enhanced to ensure that these minimise the level of security risk to the network. Specifically, filtering settings should block peer-to-peer connections from being established with user machines as well as preventing the unauthorised leakage of data from the network.
6	🟧	Our audit found that the process for data backups can be further improved to ensure the resilience and availability of the network and business data.	We recommend that, as per the requirements of the Security Policy, there is regular full-restore testing of backups i.e. the full recovery of systems on a bare-metal server using backup media. We also recommend that a formal backup plan/policy is developed to ensure a consistent approach is taken to managing backups.
7	🟧	Our audit found that currently there is no IT disaster recovery (DR) plan in place to support the recovery of infrastructure and business systems following an IT disaster.	We recommend that an IT disaster recovery plan with supporting technical recovery plans are developed to support the recovery of business critical systems following an IT disaster.
8	🟧	Our audit found that staff are able to make use of unencrypted USB devices on the network. There is a risk that Authority data may be compromised should devices be lost or stolen resulting in reputational damage and financial fines (in the context of DPA and GDPR compliance requirements).	We recommend that USB devices should be forced encrypted when first used on the network to ensure that Authority data stored on these devices is securely protected.

All our findings and recommendations are set out in the following pages and include those of low significance which have not been summarised above.

DETAILED FINDINGS AND RECOMMENDATIONS

<table>
<tr><td colspan="4">RISK: A consistent and policy driven approach has not been implemented to maintain network security.</td></tr>
<tr><th>Ref.</th><th>Finding</th><th>Sig.</th><th>Recommendation</th></tr>
<tr><td>1</td><td><b>Security Awareness Training</b>
Our audit noted that network users have not been provided with an adequate level of computer security awareness training. Also, there is no training programme in place to ensure staff understand their responsibilities with respect to protecting and securing Authority data.
With the prevalence of social engineering based attacks on computer networks and the future requirement to comply with the more stringent requirements of the General Data Protection Regulation (GDPR), there is a risk that a lack of computer security awareness within the organisation results in a network security or data breach.
The risk in this area is further heightened by the significant increase in number of ransomware attacks which are typically triggered by a network user interaction with a phishing email. This results in network files being force encrypted and a ransom being sought by attackers to unlock files.</td><td>🟧</td><td>We recommend that all users are provided with computer security awareness training. This may take the form of group-based seminars or workshops and could be supplemented by on-line test-based learning. Where possible, the subject matter should include coverage of the upcoming GDPR requirements and the potential impact of non-compliance on the Authority.</td></tr>
<tr><th colspan="3">MANAGEMENT RESPONSE</th><th>RESPONSIBILITY AND IMPLEMENTATION DATE</th></tr>
<tr><td colspan="3">Agreed. We note also the sensible suggestion to seek to combine training on security awareness with upcoming GDPR responsibilities. This training may take some time to arrange, hence the slightly longer time frame for a medium / amber level recommendation.</td><td><i>Responsible Officer: Head of Organisational Development with Governance and Corp. Performance Manager</i>
<i>Implementation Date: 31 January 2018</i></td></tr>
</table>

DETAILED FINDINGS AND RECOMMENDATIONS

RISK: There is a lack of control over how staff, third parties and other stakeholders gain access to CNPA's network.

Ref.	Finding	Sig.	Recommendation
2	**Powerful Network Access - Use of Shared Accounts** The Authority IT organisation consists of a single resource (IT Manager) with a support/backup arrangement in place with the Loch Lomond Trossachs Park Authority (LLTPA) IT department. Our audit noted that both IT organisations are making use of shared accounts to administer the network. As a result, there is no unique accountability or attribution possible with respect to these accounts. Of particular concern was shared use of the single firewall account which is used to maintain the security of the Authority network perimeter. Best practice recommends that all network accounts be uniquely assigned to ensure there is greater ownership over the security of accounts and that it is possible to maintain an effective audit trail of access and actions performed on the network. The risk is heightened with privileged accounts given that they are able to process/commit powerful (administrator level) transactions on the network and may be able to subvert security logging and monitoring controls.	🟧	We recommend that, where possible, use of shared use accounts on the network is minimised. We recommend that third party and partner support organisations (i.e. LLTPA) are set up with their own uniquely named accounts. We recommend that the password for the default firewall administrator account is changed once unique accounts are created for LLTPA and Authority IT staff.

MANAGEMENT RESPONSE	RESPONSIBILITY AND IMPLEMENTATION DATE
Agreed.	***Responsible Officer: IT Manager*** ***Implementation Date: 31 January 2018***

DETAILED FINDINGS AND RECOMMENDATIONS

<table>
<tr><td colspan="4">RISK: There is a lack of control over how staff, third parties and other stakeholders gain access to CNPA’s network.</td></tr>
<tr><th>Ref.</th><th>Finding</th><th>Sig.</th><th>Recommendation</th></tr>
<tr><td>3</td><td><b>User Account Management - Leavers</b>
Our testing of network user accounts identified a number of exceptions where leaver accounts had not been disabled/removed from the network. We were advised that this may have resulted from slow processing of paperwork by line management or HR.
There is a risk that a staff member who has left the Authority continues to gain access to the network. The risk is heightened due to staff having browser-based remote access to the network and email i.e. the network can be accessed externally using user logon credentials without the need for an Authority configured device such as a laptop/tablet.
We also noted that there is no reconciliation performed on network user accounts against a separate source of information such as payroll/HR records to identify redundant user accounts i.e. accounts that are inactive or are no longer required by staff.
As a result there is a risk that redundant network accounts could be used in order to gain unauthorised access to the network.</td><td>🟧</td><td>We recommend that network accounts for leavers are disabled as soon as the account owner leaves employment with the Authority. Controls should also ensure that accounts for temporary, agency or contract staff are disabled promptly when they are no longer required.
We also recommend that periodically a full reconciliation of user accounts is carried out by IT against an independent source of information such as HR or payroll lists to ensure only active staff members have access to the network.
Additionally, we recommend that IT periodically review accounts using last login data to identify and remove inactive accounts to minimise the risk of unauthorised access to the network.</td></tr>
<tr><th colspan="3">MANAGEMENT RESPONSE</th><th>RESPONSIBILITY AND IMPLEMENTATION DATE</th></tr>
<tr><td colspan="3">Agreed. The Head of Organisational Development will oversee a review of processes falling on from staff resignations and will also put in place arrangements for twice yearly reconciliations of user accounts against payroll.</td><td><b><i>Responsible Officer: Head of Organisational Development</i></b>
<b><i>Implementation Date: 31 January 2018</i></b></td></tr>
</table>

DETAILED FINDINGS AND RECOMMENDATIONS

RISK: Network infrastructure devices are not securely configured.			
Ref.	Finding	Sig.	Recommendation
4	**Patch Management** Our audit noted that there is currently no testing of Windows patches before these are deployed to the live environment. ManageEngine software alerts IT to the availability of patches and high priority ('critical') patches are deployed immediately without any testing to determine whether updates will have an adverse impact on the Authority network and systems. There is a risk that patches deployed to the network result in unexpected downtime for network users. We also noted that beyond the Windows server estate there is no active patch monitoring programme in place for network devices such as firewalls and routers. As a result, there is a risk that publicly known vulnerabilities in these devices may be exploited during an attack on the network.	🟧	We recommend that all patches are tested and deployed in a controlled phased manner across the server and desktop estate. We recommend that patches are first tested on a smaller group of non-business critical servers (or test servers that mirror the live environment) to assess whether these result in any adverse consequences to Authority systems before they are rolled out across the rest of the server estate. We also recommend that a patch monitoring process is implemented to take into account all network devices/appliances to ensure these are maintained in line with supplier recommended patch standards.
MANAGEMENT RESPONSE			RESPONSIBILITY AND IMPLEMENTATION DATE
Agreed.			***Responsible Officer: IT Manager*** ***Implementation Date: 31 January 2018***

DETAILED FINDINGS AND RECOMMENDATIONS

RISK: The network is not adequately protected from external threats.

Ref.	Finding	Sig.	Recommendation
5	**Web Content Filtering** Our audit found that current web content filtering settings could be further enhanced to minimise the level of risk posed to the corporate network through general user access to the internet. For example, peer-to-peer networking is currently not blocked through the Bloxx web content filtering solution. As a result, users are able to establish a direct connection with external machines to transfer/share files which could be a means to introduce viruses or other malware to the network. Also, access to cloud storage sites such as Dropbox or Google Drive has not been blocked and this increases the risk of unauthorised data leakage from the network.	🟧	We recommend that current web content filtering settings are reviewed and enhanced to ensure that these minimise the level of security risk to the network. Specifically, filtering settings should block peer-to-peer connections from being established with user machines as well preventing the unauthorised leakage of data from the network.

MANAGEMENT RESPONSE	RESPONSIBILITY AND IMPLEMENTATION DATE
Agreed. We will explore the establishment of secure file sharing arrangements to support partnership working without reliance on these much less secure current practices. In essential cases we will explore the use of Dropbox and Google Drive by authorised users on non-networked machines to minimise risk of data leakage and malware proliferation.	***Responsible Officer: Governance and Performance Manager with IT Manager.*** ***Implementation Date:*** ***31 January 2018***

DETAILED FINDINGS AND RECOMMENDATIONS

RISK: Resilience and redundancy considerations are not built into the network.

Ref.	Finding	Sig.	Recommendation
6	**Network Data Backups** Our audit found that the process for data backups can be further improved to ensure the resilience and availability of the network and business data. We noted that currently there is no testing of data backups in line with requirements set out in the IT Security Policy. This requires that backups should be tested “regularly in accordance with an agreed backup plan”. However a formal backup plan has not been defined and there has been no full restore testing of backups from tape media. Also, our testing identified more than one instance of repeat failed backups over a period of several days. There is currently no formal process in place to ensure repeat failures are root-cause investigated and re-run to ensure there are no gaps in data backup availability. There is a risk that business systems and data may not be recoverable following system failure or data corruption. The risk in this area has increased given the growing threat from ransomware attacks. Ransomware works by encrypting files/directories that can then only be unlocked by an attacker. In this situation, an organisation will generally have to default to their offline backups to recover their systems.	🟧	We recommend that, as per the requirements of the Security Policy, there is regular full-restore testing of backups i.e. the full recovery of systems on a bare-metal server using backup media. We also recommend that a formal backup plan/policy is developed to ensure a consistent approach is taken to managing backups including implementation, monitoring over their success/failure, rerunning failed backups and regular testing.

MANAGEMENT RESPONSE	RESPONSIBILITY AND IMPLEMENTATION DATE
Agreed.	***Responsible Officer: Governance and Corporate Performance Manager with IT MAnager*** ***Implementation Date: 31 January 2018***

DETAILED FINDINGS AND RECOMMENDATIONS

RISK: Resilience and redundancy considerations are not built into the network			
Ref.	Finding	Sig.	Recommendation
7	**Disaster Recovery Planning** Our audit found that currently there is no IT disaster recovery (DR) plan in place to support the recovery of infrastructure and business systems following an IT disaster. A Business Continuity Plan is in place which details 'Technology Recovery Strategies and Goals' as well as 'Internal and External (system) Dependencies'. However there is no dedicated IT DR plan in place with detailed technical recovery steps to guide the step-by-step recovery of systems. There is a risk that IT infrastructure and systems may not be recovered in an efficient and effective manner following an IT disaster and that this will have an adverse impact on the continuity of business critical operations/processes.	🟧	We recommend that an IT disaster recovery plan with supporting technical recovery plans are developed to support the recovery of business critical systems following an IT disaster. The plans should be sufficiently detailed to allow engineers that are not familiar with Authority systems to rebuild and recover servers and network hardware i.e. plans should include current configuration and systems setting information.

MANAGEMENT RESPONSE	RESPONSIBILITY AND IMPLEMENTATION DATE
Agreed.	*Responsible Officer: Governance and Corporate Performance Manager with IT Manager* *Implementation Date: 31 January 2018*

DETAILED FINDINGS AND RECOMMENDATIONS

<table>
<tr><th colspan="4">RISK: Network devices are not effectively deployed, monitored or managed.</th></tr>
<tr><th>Ref.</th><th>Finding</th><th>Sig.</th><th>Recommendation</th></tr>
<tr><td>8</td><td><b>End-Point Security - USB Devices</b>
Our audit found that staff are able to make use of unencrypted USB devices on the network. There is a risk that Authority data may be compromised should devices be lost or stolen resulting in reputational damage and financial fines (in the context of DPA and GDPR compliance requirements).
Also, as devices connecting to the network are not actively scanned, there is a risk that a virus or other malware may be introduced to user machines through USBs and then further proliferate to the rest of the network.</td><td>🟧</td><td>We recommend that USB devices should be forced encrypted when first used on the network to ensure that Authority data stored on these devices is securely protected.
We also recommend that end-point security software is used to ensure that all devices connecting to the network are security scanned.</td></tr>
<tr><th colspan="3">MANAGEMENT RESPONSE</th><th>RESPONSIBILITY AND IMPLEMENTATION DATE</th></tr>
<tr><td colspan="3">Agreed. We are conscious that these changes may cause some preliminary disruption to existing partnership working arrangements. However, this can hopefully be overcome if other more secure file sharing arrangements are identified in line with recommendation 5.</td><td><i><b>Responsible Officer: Governance and Corporate Performance Manager with IT Manager</b></i>
<i><b>Implementation Date: 31 January 2018</b></i></td></tr>
</table>

DETAILED FINDINGS AND RECOMMENDATIONS

RISK: Network infrastructure devices are not securely configured.			
Ref.	Finding	Sig.	Recommendation
9	**Security Vulnerability Testing** Our audit noted that there is currently no network vulnerability testing to assess the adequacy of the security configuration of network devices. Also, a network penetration test has not been carried out to assess the security of the network perimeter. There is a risk that network devices have been configured in an unsecure manner or that publicly known vulnerabilities exist on the network and are not been identified and remediated to ensure that these cannot be exploited to gain unauthorised access to systems. There is also a risk that the network perimeter may not be sufficiently secure to prevent unauthorised users from gaining access to the network.	●	We recommend that the network is periodically subject to vulnerability scanning, using tools such as Nessus, to ensure all known vulnerabilities are identified and corrected to prevent these from being exploited. We also recommend that management consider commissioning a network penetration test to assess the security of the external perimeter. This type of testing will deliver the most value where the Authority are reliant on delivering services over the internet, particularly those that involve payment transactions (or exchange of other sensitive data).
MANAGEMENT RESPONSE			RESPONSIBILITY AND IMPLEMENTATION DATE
Agreed. A network penetration test will be commissioned jointly with LLTNPA given the inter-dependencies of both NPA's IT networks.			***Responsible Officer: Governance and Corporate Performance Manager*** ***Implementation Date: 31 March 2018***

DETAILED FINDINGS AND RECOMMENDATIONS

<table>
<tr><th colspan="4">RISK: Network infrastructure devices are not securely configured.</th></tr>
<tr><th>Ref.</th><th>Finding</th><th>Sig.</th><th>Recommendation</th></tr>
<tr><td>10</td><td><b>Establishing a Security Baseline</b>
Our audit found that the IT security control environment could be improved through introducing minimum security baselines for network builds.
Currently network devices such as servers, routers and switches are configured without any formal reference to recommended security guidelines, such as those defined through organisations such as CIS (Centre for Internet Security). These baselines act as checklists ensuring devices are configured to a minimum security standard in line with best-practice industry recommendations.
There is a risk that network devices may not be effectively hardened (i.e. locked down) and secured before being deployed to the live environment.</td><td>●</td><td>We recommend that all network devices are configured with reference to recognised security baselines to ensure that all active network components have met a minimum security standard.</td></tr>
<tr><th colspan="3">MANAGEMENT RESPONSE</th><th>RESPONSIBILITY AND IMPLEMENTATION DATE</th></tr>
<tr><td colspan="3">Agreed.</td><td><i><b>Responsible Officer: IT Manager</b></i>
<i><b>Implementation Date: 31 March 2018</b></i></td></tr>
</table>

DETAILED FINDINGS AND RECOMMENDATIONS

RISK: Security incident monitoring and response procedures are ineffective.

Ref.	Finding	Sig.	Recommendation
11	**Security Monitoring & Logging** Our audit found that there is no formal strategy in place with respect to security logging and monitoring on the network. There is default logging in place on the network for certain devices such as the firewall and logging of certain events through Active Directory. However, these have been enabled as default settings and not through well thought out security design. We found that with most of these, settings logs are quickly overwritten and are not subject to any form of security monitoring or analysis. There is a risk that potential or actual network security violations are not detected and actioned by the Authority. Also, given the upcoming GDPR compliance deadline of May 2018, there is a risk that without sufficient levels of monitoring and tracking of sensitive data, the Authority will not be able to demonstrate adequate levels of compliance with Regulation requirements.	●	We recommend that the Authority consider developing and implementing a network security monitoring and logging strategy to ensure that areas of the network that are used to store or process sensitive data are subject to proactive monitoring controls. Also, we recommend that management consider introducing a syslog for securely capturing and retaining log information to ensure the availability and integrity of log data is maintained.

MANAGEMENT RESPONSE	RESPONSIBILITY AND IMPLEMENTATION DATE
Agreed.	***Responsible Officer: IT Manager*** ***Implementation Date: 31 March 2018***

APPENDIX I - STAFF INTERVIEWED

NAME	JOB TITLE
Sandy Allan	IT Manager
Helen Rees	Governance and Corporate Performance Manager
Pip Mackie	HR Support Officer

BDO LLP appreciates the time provided by all the individuals involved in this review and would like to thank them for their assistance and cooperation.

APPENDIX II - DEFINITIONS

LEVEL OF ASSURANCE	DESIGN of internal control framework		OPERATIONAL EFFECTIVENESS of internal controls	
	Findings from review	Design Opinion	Findings from review	Effectiveness Opinion
Substantial 🟢	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
Moderate 🟦	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non compliance with some controls, that may put some of the system objectives at risk.
Limited 🟠	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
No 🔺	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non compliance and/or compliance with inadequate controls.

Recommendation Significance	
High 🔺	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
Medium 🟧	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
Low 🟢	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.

APPENDIX III – TERMS OF REFERENCE

BACKGROUND

Cairngorms NPA is reliant on its ICT infrastructure and business systems to deliver services effectively to internal and external stakeholders. As part of the 2016-17 Internal Audit Plan, it was agreed that Internal Audit that we would carry out an assessment of the general technology control environment by considering the adequacy of network security at both the logical and physical layers. We will also assess arrangements in place for the monitoring, maintenance and administration of the network and network devices. A core part of our review will be to assess the level of resilience and redundancy built into the network by considering network availability, data backups and ICT disaster recovery planning. We will also review the adequacy of service desk arrangements including incident, change and performance management.

PURPOSE OF REVIEW

The purpose of the review is to assess the general controls in place in relation to information technology. The review will focus on physical and logical access controls, system support arrangements, and program change controls.

KEY RISKS

Based upon the risk assessment undertaken during the development of the internal audit operational plan, through discussions with management, and our collective audit knowledge and understanding, the key risks associated with the area under review are:

- A consistent and policy driven approach has not been implemented to maintain network security;
- There is a lack of control over how staff, third parties and other stakeholders gain access to CNPA's network;
- Network infrastructure devices are not securely configured;
- Network devices are not effectively deployed, monitored or managed;
- The network is not adequately protected from external threats;
- Resilience and redundancy considerations are not built into the network; and
- Security incident monitoring and response procedures are ineffective.

www.bdo.co.uk