Internal Audit

Network Management

March 2018

Internal Audit Assurance assessment:

Objective One	Objective Two	Objective Three	Objective Four
Significant assurance	Limited assurance	Significant assurance	Significant assurance

Timetable

Date closing meeting held: 24 November 2017

Date draft report issued: 2 March 2018

Date management comments received: 28 March 2018

Date Final report issued: 3 April 2018

Date presented to Audit and Risk Committee: 23 April 2018

Introduction

The key objectives of network management are security, performance, and reliability. Effective security is essential to prevent unauthorised and malicious access to the system, e.g. the recent ransomware attack which affected boards across NHS Scotland. Security also includes steps taken to prevent users from accessing certain websites and using certain peripherals, e.g. thumb drives.

Network performance management should ensure that system bottlenecks are anticipated and resolved in a timely manner, and that there is sufficient capacity for all users. Those responsible for network reliability should ensure that downtime is minimised and, where it is necessary, it occurs during off-peak periods. In addition, any unexpected problems should be dealt with in a timely manner.

NHS Lothian's network management and network security teams use a variety of software packages to manage the system, e.g. SolarWinds which monitors network performance, and FireSIGHT which oversees network security.

Scope

The objective of the audit was to evaluate the design and effectiveness of the key internal controls over network management and network security. The audit did not cover controls over physical security.

Acknowledgements

We would like to thank all staff consulted during this review, for their assistance and cooperation.

Executive Summary

Summary of Findings

The table below summarises our assessment of the risks and the adequacy and effectiveness of the controls in place to meet each of the risk areas agreed for this audit. Definitions of the ratings applied to each action are set out in Appendix 1.

No.	Control Objectives	Assurance Level	Number of findings			
			Critical	High	Medium	Low
1	The network is efficient and reliable, so providing an effective service for users.	Significant assurance	-	-	-	1
2	Network security is effective, to prevent unauthorised and malicious access to the system.	Limited Assurance	-	1	-	-
3	There is effective reporting on network performance and security to committee.	Significant assurance	-	-	-	-
4	There is an effective process for resolving problems, including root cause analysis.	Significant assurance	-	-	-	-
TOTAL			**-**	**1**	**-**	**1**

Conclusion

The area under review comprised four control objectives, of which three received Significant Assurance and one received Limited Assurance.

There is medium term planning in place for eHealth through the *Technical Services Strategy*, there is effective regular reporting of network performance and security statistics to eHealth management. However, there is no regular checking of access rights for users for the network management and network security systems, to confirm that access rights are appropriate and are only provided to current members of staff.

Main Findings

NHS Lothian's eHealth *Technical Services Strategy* sets out the current IT resources, and proposed future resources with the expected future costs for each key system, e.g. email, TrakCare, and system back-ups. In addition to timely updates and patches to systems there is regular, effective reporting of network performance and security statistics to eHealth management. Also, a penetration test of the firewall was conducted in 2017. We noted that although eHealth does produce major incident reports, for example the power outage at the Royal Infirmary of Edinburgh in 2016, no report was produced for the WannaCry ransomware attack in 2017. eHealth stated that one was not produced for this incident as it was a near miss and that their tools behaved as expected and safeguarded the organisation.

However, we identified one key finding for improvement during the review:

- At present there is no regular checking of access rights for users for the network management and network security systems, to confirm that access rights are appropriate and are only provided to current members of staff. A review of the access rights for the IT network management and security software systems showed that one member of staff, who left the organisation over 5 years ago, still had admin access for the Symantec Messaging Gateway software. However, system logs for this software showed that the user had not accessed this system once he had departed the organisation.

Further details of this point and one Low finding are set out in the Management Action Plan.

Management Action Plan

<table>
<tr><td>Control objective 1: The network is efficient and reliable, so providing an effective service for users.

Finding: eHealth’s Technical Services Strategy was not approved by committee in a timely manner</td><td>Low</td></tr>
<tr><td colspan="2">Observation and risk

Long- and medium-term planning for IT systems is vital to help ensure that they will continue to meet the needs of users and help achieve wider organisational objectives.

NHS Lothian’s eHealth Technical Services Strategy sets out the current IT resources, and proposed future resources with the expected future costs for each key system, e.g. email, TrakCare, and system back-ups. However, the Strategy was in draft for over 6 months before being approved in December 2017.

If strategies are not formally agreed in a timely manner then there is an increased risk that plans for the forthcoming three to five year period cannot be started.

If the future IT needs of the organisation are not agreed and planned for, there is an increased risk that the implementation of plans is delayed affecting, for example, the time taken to recruit necessary staff and upgrade systems.</td></tr>
<tr><td colspan="2">Recommendation

Draft eHealth policies and procedures should be approved by a senior committee in a timely manner.</td></tr>
<tr><td colspan="2">Management Response

eHealth agree that the strategy took some time to create, primarily as a result of changing national requirements and the need to take cognisance of these. To ensure that the strategy is always aligned to a rapid developing technical landscape there is a 6 monthly review as part of that strategy.

The Management Action

eHealth Management agree to review the strategy as set out in the document.</td></tr>
<tr><td>Responsibility:

Head of eHealth Operations & Infrastructure</td><td>Target date:

31/03/2018</td></tr>
</table>

Control objective 2: Network security is effective, to prevent unauthorised and malicious access to the system. **Finding: A former NHS Lothian staff member still had admin access for the Symantec Messaging Gateway software**	**High**

Observation and risk

When staff leave the organisation their access rights for IT systems should be removed. This process is performed by the eHealth Directory Services team and, for more specialist IT systems, by the relevant eHealth team.

However, a review of the admin access rights for all staff for all IT network management and security software systems showed that one member of staff, who left the organisation over 5 years ago, still had admin access for the Symantec Messaging Gateway software. The Senior Technical Project Manager stated that the staff member's access rights had not been removed due to an administrative oversight.

The Senior Technical Project Manager further stated that access to the overall NHS Lothian network is automatically suspended for individual users if they have not accessed the network for a period of 3 months. Therefore, the user mentioned above will not have had access to any NHS Lothian system after this 3-month period had elapsed. System logs for the Symantec Messaging Gateway software showed that the user had not accessed this system once he had departed the organisation.

At present there is no regular checking of access rights for users for the network management and network security systems, to confirm that access rights are appropriate and are only provided to current members of staff.

If access rights for users are not regularly reviewed there is an increased risk that network management and security systems are inappropriately accessed.

Recommendation

Users' access rights for all network management and security software systems should be checked every quarter to confirm that access rights are appropriate.

Management Response

A clearly documented and followed processes exist for suspension of accounts of staff who leave NHS Lothian. However there is a requirement for eHealth to put in additional control steps when staff leave Technical Services.

The Management Action

The eHealth Management team agree that an additional process is required, and we will develop a Standard Operating Procedure to check all the System Administration Tools each

time a member of Technical staff leaves this team.	
Responsibility: Head of eHealth Operations & Infrastructure	Target date: 30/04/2018

Appendix 1 - Definition of Ratings

Findings and management actions ratings

Finding Ratings	Definition
Critical	A fundamental failure or absence in the design or operating effectiveness of controls, which requires immediate attention
High	A key control failure has been identified which could be either due to a failure in the design or operating effectiveness. There are no compensating controls in place, and management should aim to implement controls within a calendar month of the review.
Medium	A control failure has been identified which could be either due to a failure in the design or operating effectiveness. Other controls in place partially mitigate the risk to the organisation, however management should look to implement controls to fully cover the risk identified.
Low	Minor non-compliance has been identified with the operating effectiveness of a control, however the design of the control is effective

Report ratings and overall assurance provided

Report Ratings	Definition	When Internal Audit will award this level
No assurance	The Board cannot take any assurance from the audit findings. There remains a significant amount of residual risk.	The controls are not adequately designed and / or operating effectively and immediate management action is required as there remains a significant amount of residual risk(for instance one Critical finding or a number of High findings)
Limited assurance	The Board can take some assurance from the systems of control in place to achieve the control objective, but there remains a significant amount of residual risk which requires action to be taken.	This may be used when: • There are known material weaknesses in key control areas. • It is known that there will have to be changes that are relevant to the control objective (e.g. due to a change in the law) and the impact has not been assessed and planned for. The controls are deficient in some aspects and require management action (for instance one 'high' finding and a number of other lower rated findings)

Moderate assurance	The Board can take reasonable assurance that controls upon which the organisation relies to achieve the control objective are in the main suitably designed and effectively applied. There remains a moderate amount of residual risk.	In most respects the "purpose" is being achieved. There are some areas where further action is required, and the residual risk is greater than "insignificant". The controls are largely effective and in most respects achieve their purpose with a limited number of findings which require management action (for instance a mix of 'medium' findings and 'low' findings)
Significant assurance	The Board can take reasonable assurance that the system(s) of control achieves or will achieve the control objective. There may be an insignificant amount of residual risk or none at all.	There is little evidence of system failure and the system appears to be robust and sustainable. The controls adequately mitigate the risk, or weaknesses are only minor (for instance a low number of findings which are all rated as 'low' or no findings)