Internal Audit

IT Applications

November 2018

Internal Audit Assurance Assessment:

Objective One	Objective Two	Objective Three	Objective Four	Objective Five
Moderate Assurance	Significant Assurance	Significant Assurance	Significant Assurance	Significant Assurance

Timetable

Date closing meeting held: No meeting held, client responded directly to draft report

Date draft report issued: 28 September 2018

Date management comments received: 8 October 2018

Date Final report issued: 1 November 2018

Date presented to Audit and Risk Committee: 26 November 2018

Contents

1. Introduction

1.1 NHS Lothian relies on clinical IT systems to ensure the safe and effective delivery of care. As part of our strategic internal audit planning process, we include in our plans an annual review of certain controls over key IT application.

1.2 NHS Lothian currently has 55 clinical applications with a total of 144,050 users. There are 22 applications categorised by as high priority as their operation is essential to the day-to-day operations of NHS Lothian. The number of users of these applications range from 18,000 (SCI Gateway) to 20 (CHEMOCARE, RHSC chemotherapy management).

Scope

1.3 The objective of the audit was to evaluate controls governing hardware and operating systems used to run NHS Lothian's clinical IT applications, including how changes and fixes to applications, servers and operating systems are managed.

Acknowledgements

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

2. Executive Summary

Summary of Findings

2.1 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	Key systems and data are protected in the event of failure or breakdown.	Moderate Assurance	-	-	1	1
2	Unauthorised access to and amendment of operating systems is prevented.	Significant Assurance	-	-	-	-
3	Measures are in place to ensure that data is effectively protected from unauthorised access and/or amendments.	Significant Assurance	-	-	-	1
4	All software amendments, upgrades and fixes are adequately assessed tested and authorised prior to application to the live environment.	Significant Assurance	-	-	-	-
5	Key Hardware is regularly maintained in order to avoid unnecessary disruption of services	Significant Assurance	-	-	-	-
TOTAL			**-**	**-**	**1**	**2**

Conclusion

2.2 There is a reasonable framework of control in ensuring that key application data is being backed up regularly and servers used for the storage of the data operating effectively and protected against system failure or data loss. Adequate controls are also in place to ensure that changes to applications are subject to review, approval, testing before implementation.

Main Findings

2.3 System resilience has been built in through the use of multiple power supplies, with uninterrupted power supply also in place to ensure that power to the computer servers is maintained.

2.4 Larger applications, such as Trak, iLabs and sci store have full fallover support. Data is mirrored across servers in separate locations and in the event of one failing, the application can be run effectively from the other.

2.5 Clinical systems are being backed up to a predetermined schedule and parameters. With software in place to monitor backup completion and notify eHealth staff where failed backups have occurred. The operation and effectiveness of the back-up software is monitored in addition to the performance of the relevant hardware.

2.6 Similarly, programmes are operating to monitor the functionality of the servers and notify staff where server temperature is excessive or service processes or applications are affected. Functional effectiveness of the equipment used is monitored, with an alert system in place where failures or other issues occur.

2.7 Servers used to store application data are contained within secure environments with access granted only to authorised personnel.

2.8 Applications and operating systems are subject to effective controls around fixes, changes and patching with a Change Advisory Board in place to review and approve all application changes prior to implementation to the live environment.

2.9 We identified four issues / improvement opportunities during this review:

<u>Medium Rating</u>

- While the server backup schedule is documented, there are no controls around the review, update and approval of the schedule. Also, the process for identifying and resolving a failed backup has not been documented into a standard operating procedure or similar.

<u>Low Rating</u>

- The arrangements for storing back-up tapes are not entirely compliant with best practice, which requires that contents of back-up stores are checked regularly to ensure that the required data is available and that the Board's retention policies followed. Storage locations should themselves be secure, accessible only by authorised staff and protected from environmental damage.

- During data centre walk rounds at the WGH and SJH, it was noted that the folder for documenting staff activity in one of the server rooms at SJH was not being used and consequently there are insufficient records of who has accessed the room should issues occur with the loss, damage or unauthorised access to servers and the data held therein.

3. Management Action Plan

Finding 1	
Control objective 1: Key systems and data are protected in the event of failure or breakdown. **Associated risk of not achieving the control objective: Backup tapes are at risk of loss or damage.**	**Low**

Background

eHealth have several data centres located across a number of sites. They are used to house servers for the storage of all data required for the effective operation of the Board's clinical and non-clinical software applications.

All data centres are subject to appropriate operational and environmental controls, including uninterrupted power supplies, fire suppression and CCTV. Additionally, programmes are operating to monitor the room environment and notify staff where temperatures are out with acceptable limits.

In addition to backing up data to other servers, eHealth staff continue to back up to tape and this task is carried out within the server rooms. Staff are then required to store the tapes at a location separate to the server rooms though still subject to reasonable security and environmental controls.

Observation and risk

During data centre walk rounds, it was noted that the arrangements for storing back-up tapes are not entirely compliant with best practice. The location used at the WGH is being kept secure, however the tapes are not subject to appropriate controls to prevent their damage from fire or flood. Also, a number of tapes held are dated as far back as 2012, which may not comply with the Boards policy on the retention and destruction of data.

Also, the tape storage location at the SJH could not be assessed during fieldwork as the location and keys for accessing are known one member of staff, who was off on leave at the time.

- Contents of backup store checked regularly to ensure that the required files are available.
- Store is adequately protected by alarms etc
- Compliance with relevant data retention legislation and NHSL policies.
- Key system back-up media are checked periodically to ensure that the contents remain readable.

Recommendation

Management should carry out a review of all locations used for the storage of back-up tapes. This should include a review of the controls preventing environmental damage and loss or

theft (security), including access to the site and key storage. This review should also include a reconciliation of all tapes and those no longer required should be securely disposed of.	
Management Response Mangement accept that improvement can and needs to be made with regards to storage of backup tapes. However it should be noted that with the recent introduction of new backup appliances giving an additional 500TB of backup space there are moves in place already to move backups away from tape drives. The Management Action eHealth management will review the current procdures with regards to storate and retention of backup tapes, and develop and implement a standard operating procedure taking into account the points raised in this audit.	
Responsibility: Technical Services Manager	Target date: 31 December 2018

Finding 2	
Control objective 1: Key systems and data are protected in the event of failure or breakdown. **Associated risk of not achieving the control objective: Backup failure may not be adequately resolved.**	**Medium**

Background

Server to server backup is being carried out automatically according to a predetermined schedule and parameters. Backups are monitored using Symantec NetBackup administration software. The operation and effectiveness of the back-up software and performance of the relevant hardware is monitored by eHealth staff.

eHealth staff are notified by system-generated email of backups only on an exception basis, such as where a backup has failed to complete.

A member of staff will then look into the issue and take the necessary action to resolve it.

Observation and risk

While the server backup schedule is documented, there are no controls around the review, update and approval of the schedule. And as such it cannot be confirmed that it is valid, up-to-date and contains accurate backup information.

Also, the process for identifying and resolving a failed backup has not been documented into a standard operating procedure or similar. Because of this staff may be unclear on who has taken responsibility for certain tasks and whether they have been resolved.

Recommendation

Management should put in place a process to review the server backup schedule to ensure that it remains relevant. It is suggested that this is subject to annual review and following any changes.

Also the procedures followed for allocating work around correcting server backup failures should be documented, and daily / weekly checks undertaken to confirm that the Symantec NetBackup is operating as expected.

Management Response

Management acknowledge that there is room for improvement and that additional controls should be established with regards to implementation and changes of the backup software.

The Management Action

eHealth will develop and implement a standard operating procedure to cover the review of implementation and changes of backup schedules.

Responsibility:	Target date:
Technical Services Manager	31 December 2018

Control objective 2: Unauthorised access to and amendment of operating systems is prevented.
We identified no significant weaknesses in relation to this control objective. Currently, eHealth technical services staff use two accounts for accessing NHS Lothian's IT infrastructure. One is a 'working' non-administrator account for carrying out their day-to-day operations and the second is an elevated, or privileged access account, which provides additional access and rights above the 'normal' account. A privileged access account allows non-restrictive access to operating systems where users can perform a wide array of actions, including browsing and downloading programs from the web. All eHealth engineers with elevated accounts access these accounts using individual usernames and passwords which are separate from the access details for their non-administrator accounts. Appropriate controls are in place to monitor the elevated accounts operations, should management be required to identify any inappropriate activity.

Finding 4	
Control objective 3: Unauthorised access to and amendment of operating systems is prevented. **Associated risk of not achieving the control objective: Senior staff may be unable to identify individuals that have recently accessed server rooms.**	**Low**
Background In addition to CCTV, access to data centres is controlled through the use of proximity cards with staff also required to sign in and out using documentation held within the data centres. Observation and risk During data centre walk rounds at the WGH and SJH, it was noted that the folder for one of the server rooms at SJH was not being used and consequently there are insufficient records of who has accessed the room. Should any issues occur with the operating systems, senior staff may be unable to identify individuals that have recently accessed the server room and could be responsible.	
Recommendation Management should remind staff of the requirement to maintain effective records of who is accessing the server rooms. This should be supported by occasional walkround to ensure that this is being done and that the general environment within the rooms is acceptable.	
Management Response Each server room has proximity card access. The logs are reviewed by the security team on an annual basis to make sure only appropriate staff have access to the room. In addition each server room has an environmental monitoring solution, which includes a motion activated camera which captures who is ever in the room. These are extra measures which don't appear to be mentioned in the audit as mitigating the risk of not completing the room logs. The Management Action The management team will make sure that the logs are kept up to date as per the agreed process.	
Responsibility: Technical Services Managers	Target date: 31 October 2018

Control objective 4: All software amendments, upgrades and fixes are adequately assessed, tested and authorised prior

We identified no significant Issues in relation to this control objective.

An eHealth Change Management procedure is in place and being followed for requests for change, all of which are processed through the Assyst IT support service.

In the first instance the eHealth service or Technical Manager logs requests for change on Assyst. Once done, the Change Manager is notified by the system and a record made of this request in a separate change control tracker spreadsheet.

All change requests received during the week are compiled and presented to the Change Advisory Board (CAB) each Monday, where they are reviewed and, if approved, assigned to a relevant member of eHealth.

Once changes are authorised, the CAB allocates priority, start and end dates to gfit in with eHealth planned schedule of work. All changes are tested within a controlled environment and released into the live environment only once the CAB has conducted a review and sign-off of the change.

The request for change is then closed off on Assyst.

A standard operating procedure (SOP) for server operating system patching is in place and followed by eHealth staff. The SOP clearly documents the process and procedure for patching the operating system of all servers across the NHS Lothian estate.

Control objective 5: Key Hardware is regularly maintained in order to avoid unnecessary disruption to services.

We identified no significant weaknesses in relation to this control objective.

Server functionality and performance is monitored automatically using an open-sourced software programme called Nagios.

Server monitoring through Nagios has provided a number of benefits to the organization:

- Increased server, services, process, and application availability.
- Fast detection of network and server outages and protocol failures.
- Fast detection of failed servers, services, processes and batch jobs.

Applications are also being monitored through this software to detect application or process problems.

Also, servers are being regularly updated following the receipt of Microsoft's security bulletin.

The Senior Server Engineer emails all relevant staff advising them of the most recent Microsoft update and when to expect servers to have scheduled downtime

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)