NHS Lothian
Internal Audit Report 2021/22
IT Asset Management

Assurance Rating: Significant Assurance

Date 9 June 2022

Final Report

Contents

The contacts in connection with this report are:

Joanne Brown
Partner
T: 0141 223 0848
E: joanne.e.brown@uk.gt.com

Peter Clark
Director, Public Sector Internal Audit
T: 0141 223 0785
E: peter.c.clark@k.gt.com

Russell Richmond-McIntosh
Principal Auditor
T: 0131 465 7757
E: Russell.mcintosh@nhslothian.scot.nhs.uk

Timetable

- Date closing meeting held: Client responded directly to draft report
- Date draft report issued: 8 June 2022
- Date management comments received: 9 June 2022
- Date Final report issued: 9 June 2022
- Date presented to Audit and Risk Committee: 20 June 2022

Executive Summary

Introduction

NHS Lothian's main assets can be split into five groups, one of which is eHealth (hardware and infrastructure) which had a NPV of £4.3m at 31 March 21. Due to the pandemic, and the move towards working from home, IT asset management including the process of accounting for, maintaining, upgrading and disposing of assets has become of vital importance.

Within NHS Lothian, IT assets can be broken down into two categories; high value items and items utilised by the client/end user. An audit completed pre-pandemic focused on high value items, therefore, this audit will primarily focus on client/end user assets and the controls in place around these assets.

NHS Lothian utilises Microsoft System Centre Configuration Manager (SCCM) for the management, deployment and security of devices and applications across the organisation. However, for assets which are held by the end user, (which have increased during the pandemic due to individuals working from home) on a six-monthly basis, the user is required to provide an update on where the assets are held, which feeds into the Asset Management system. There are manual processes in place and where assets are commissioned/decommissioned, and the Directory must be manually updated to reflect.

Scope

The objective of the audit is to evaluate the adequacy of internal controls in place around IT Asset Management and review the design and operating effectiveness of the controls to mitigate against the following potential risk areas:

- There is a lack of knowledge and expectations over the asset management process and as a result, assets are not effectively managed.
- There is limited or no oversight to ensure the recording of assets is complete and on a timely basis, resulting in commissions/ decommissions not being recorded.
- The process in place for monitoring the location of an asset is not complied with and the asset is not being used in a compliant manner, resulting in NHS Lothian being unaware of each asset's location and increasing the risk of a data security breach by the end user.

Acknowledgments

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

Limitations in Scope

Please note that our conclusion is limited by scope. It is limited to the risks outlined above. Other risks that exist in this process are out with the scope of this review and therefore our conclusion has not considered these risks. Where sample testing has been undertaken, our findings and conclusions are limited to the items selected for testing.

This report does not constitute an assurance engagement as set out under ISAE 3000.

Summary of Findings

We have concluded that the controls in place in respect of the reporting, decision making and collaboration in relation to IT Asset Management provides a **SIGNIFICANT** level of assurance. The table over the page provides a summary of the findings. The ratings assigned are based on the agreed internal audit rating scale (**Appendix 2**).

Detailed findings, recommendations and agreed management actions are found in Section 2 of this report.

SIGNIFICANT assurance

Summary of Processes followed and controls

Several procedures are in place to guide staff on the appropriate use and management of IT assets, This includes the NHS Lothian Digital Technical Services Standard Operating Procedure - Device Management and NHS Lothian Digital IT Security Policy. All policies are up-to-date and readily available for staff to refer to.

The Head of Digital Operations and Infrastructure and other relevant staff within eHealth utilise Microsoft System Centre Configuration Manager (SCCM) to access the monthly KPI client count, which provides real time information on the number of assets in the active directory at any given time.

On desktop devices managed by SCCM, the Location Inventory records data entered by the user and automatically runs every January, or when a new device is added to the domain. Where information provided is inaccurate, eHealth can track the location of the asset using its unique IP address.

In addition to a hardware and software inventory, SCCM provides remote control, patch management, software distribution, operating system deployment and network access. Testing identified no areas of control weakness in these areas.

eHealth run a monthly vulnerability scan on all devices. Where vulnerabilities in packages are identified, they are either updated or removed.

NHS Lothian uses encryption to ensure the security of mobile devices. NHS Lothian approved devices are configured so that unauthorised users cannot gain access to them.

Executive Summary

HIGH	MEDIUM	LOW	ADVISORY
-	-	1	-

Ref	Issue	H	M	L	A
2.1	The IT Security LearnPro training module is incomplete for a number of staff	-	-	1	-
TOTAL		-	-	1	-

Follow Up

Approximately two weeks following issue of the final Internal Audit report, a member of the Audit Team will issue an 'evidence requirements' document for those reports where management actions have been agreed. This document forms part of the follow up process and records what information should be provided to close off the management action.

The follow-up process is aligned with the meetings of the Board's Audit & Risk Committee. Audit Sponsors will be contacted on a quarterly basis with a request to provide the necessary evidence for those management actions that are likely to fall due before the next meeting of the Audit and Risk Committee.

Management Action Plan

Finding 2.1 – The IT Security LearnPro training module is incomplete for a number of staff	LOW

Control

All new staff receive basic IT training at induction and are required in all instances to sign the NHS Lothian eHealth user access form, Signing of this form demonstrates compliance with the NHS Lothian eHealth Security Policy and confidentiality requirements. Staff are expected to have read the eHealth Statement on the reverse of the form and understand that they are responsible for all transactions carried out under their User ID.

All staff are also required every two years to complete the mandatory LearnPro module - Information Governance, which includes IT security. The IT Security module is split into 5 sections and includes NHS Lothian IT System, and IT equipment / removeable media.

Staff are advised through the module to not leave any device lying around out with the workplace and keep them locked and out of sight if carrying in a vehicle.

In April 2021, NHS Lothian introduced the LearnPro Scorecard as the new tool for monitoring and reporting compliance with core mandatory and role-essential training. The Scorecard provides line managers with real-time measurement of mandatory compliance, through a colour-coded dashboard.

Observation

As at 19 May 2022, the Information Governance module completion was 71% for NHS Lothian as a whole, and 85% for eHealth. NHS Lothian's Learning & Development Strategy requires that 80% of staff have undertaken all their mandatory training requirements.

These figures don't include face to face training provided to staff (on department request) that do not have a LearnPro account. Therefore with those staff included, the total figure is likely to be higher than 71%, although still lower than 80%

Risk

While the completion of the Information Governance modules is above the 80% threshold for eHealth staff, there is a risk that without reasonable awareness of the NHS Lothian policies and good practice surrounding IT Security, staff elsewhere are not adhering to the guidance and exposing IT equipment to unauthorised use, loss or theft.

Recommendation
Management should be advised of the importance of completing the NHS Lothian core mandatory learning modules and utilise the LearnPro Scorecard to identify and act upon instances of non-compliance within their area.

Management Response
Accepted. It should be noted that during the pandemic most training was stood down as we started to re-commence training the decision of the Corporate Management Team was to prioritise mandatory training for fire safety and HAI. CMT have now agreed that for the performance year 2022/23 80% compliance across all mandatory subjects, including Information Governance is expected.

Management Action
New LearnPro reporting tools have now been launched which will make it easier for managers to access performance data for their teams and to target improvements actions and there have been recent communications to this effect to line managers and in Team Brief for all mandatory training subjects. There will be communications throughout the year to raise awareness and importance of mandatory training.

Responsibility:	Target Date
Director of HR & OD	31 October 2022

Appendices

Appendix 1 – Staff Involved and Documents Reviewed

Staff Involved

- Head of Digital Operations and Infrstructure
- Technical Services Manager

Documents Reviewed

- Digital Technical Services Device Management Standard Operating Procedure
- Digital IT Security Policy
- NHS Lothian Home Working Policy
- Working from Home – Information Governance Policy Statement
- Digital Technical Services Digital System & Domain Administrator Accounts Standard Operating Procedure
- Digital Technical Services Vulnerability Scanning Standard Operating Procedure
- IT Asset Client count as at 20 May 2022
- NHS Lothian User ID Request Form
- Windows 10 - LUHT imaging Instructions
- Active Directory Asset Removal Guide
- Secure Storage Disposal and Destruction of Electronic Equipment Policy
- NHS Lothian Line Manager Scorecard Guide

Appendix 2 – Our IA Report assurance levels

The table below shows the levels of assurance we provide and guidelines for how these are arrived at. We always exercise professional judgement in determining assignment assurance levels, reflective of the circumstances of each individual assignment.

Rating	Definition	When Internal Audit will award this level
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)
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)
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)
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)

Appendix 2 - Continued

The table below describes how we grade our audit recommendations based on risks

Rating	Description	Possible features
High	Findings that are fundamental to the management of risk in the business area, representing a weakness in the design or application of activities or control that requires the immediate attention of management	▪ Key activity or control not designed or operating effectively ▪ Potential for fraud identified ▪ Non-compliance with key procedures / standards ▪ Non-compliance with regulation
Medium	Findings that are important to the management of risk in the business area, representing a moderate weakness in the design or application of activities or control that requires the immediate attention of management	▪ Important activity or control not designed or operating effectively ▪ Impact is contained within the department and compensating controls would detect errors ▪ Possibility for fraud exists ▪ Control failures identified but not in key controls ▪ Non-compliance with procedures / standards (but not resulting in key control failure)
Low	Findings that identify non-compliance with established procedures, or which identify changes that could improve the efficiency and/or effectiveness of the activity or control but which are not vital to the management of risk in the business area.	▪ Minor control design or operational weakness ▪ Minor non-compliance with procedures / standards
Advisory	Items requiring no action but which may be of interest to management or which represent best practice advice	▪ Information for management ▪ Control operating but not necessarily in accordance with best practice


Grant Thornton
NHS
Lothian