Grant Thornton

NHS Lothian

Internal Audit 2023/24

Information Security–Follow-up

February 2024

Final Report

Emily Mayne
Head of Internal Audit
T 0121 232 5309
E emily.j.mayne@uk.gt.com

Jamie Fraser
Internal Audit Assistant Manager
T 0141 223 0886
E jamie.a.fraser@uk.gt.com

Matt Lee
Assistant Manager
T 0121 232 8784
E matt.d.lee@uk.gt.com

Contents

This report is confidential and is intended for use by the management and directors of NHS Lothian. It forms part of our continuing dialogue with you. It should not be made available, in whole or in part, to any third party without our prior written consent. We do not accept responsibility for any reliance that third parties may place upon this report. Any third party relying on this report does so entirely at its own risk. We accept no liability to any third party for any loss or damage suffered or costs incurred, arising out of or in connection with the use of this report, however such loss or damage is caused.

It is the responsibility solely of NHS Lothian management and directors to ensure there are adequate arrangements in place in relation to risk management, governance, control and value for money.

Report Distribution

Executive Lead:

- Martin Egan, Director of Digital

For action:

- Iain Robertson, Head of eHealth Operations and Infrastructure

For Information:

- Calum Campbell - Chief Executive
- Craig Marriott, Director of Finance
- Tracey McKinley, Information Governance and Security Manager
- Audit and Risk Committee

Executive summary

Background

This follow-up audit on Information Security was conducted to review the implementation actions taken by NHS Lothian in response to the recommendations identified in the 2022/23 Information Security Internal Audit review. Our focus was on evaluating progress made in implementing the agreed recommendations and assessing the supporting evidence to confirm their implementation status. The recommendation areas from the original report included asset management, access control, user engagement, and incident response.

The methodology for this follow-up comprised interviews, and documentation reviews. This report provides an updated position of NHS Lothian's progress in mitigating prior weaknesses and identified areas which required attention.

Objectives

Our review focussed on the following key risk:

- Failure to implement recommended actions from the 2022/23 Information Security Internal Audit report may indicate insufficient commitment or resources dedicated to information security.

Limitations in scope

Please note that our conclusion is limited by scope. It is limited to the risks outlined above. Our implementation assessments are based solely on the follow-up information and evidence provided by the Board and relate to the associated risks identified in our 2022/23 review. Other risks exist in this process which our review and therefore our conclusion has not considered.

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

Acknowledgement

We would like to take this opportunity to thank your staff for their co-operation during this internal audit.

Headline messages

Conclusion

Significant Assurance

We have examined the implementation progress of the five management actions agreed in the 2022/23 Information Security Internal Audit report, which originally received a Moderate Assurance rating. Although full implementation is yet to be achieved, the progress made so far has reduced the risks identified in our original report. As a result, we have updated our current Assurance Rating to Significant Assurance recognising that there is still action to be taken.

Two out of the five actions have been successfully implemented, and progress has been made on the remaining three. Notable advancements include the implementation of updated policies and procedures. Nevertheless, it is important that NHS Lothian maintains momentum in completing the remaining actions and consistently reviews its security protocols to safeguard against evolving cyber threats.

The below table summarises the current implementation status of the five agreed actions from the 2022/23 Information Security Internal Audit review. Individual details are recorded in the ‘Detailed Findings’ of this report.

Action Reference and Title	2022/23 Rating	Action Status	2023/24 Rating
2.1 - Continuation of Planned Replacement Programs	Medium	In Progress (Not Due)	Low
2.2 - Azure Password Policy Update	Medium	Implemented	N/A
2.3 - Establishment of Standard Operating Procedure	Medium	In Progress (Over Due)	Low
2.4 - New Password Policy for Privileged Accounts	Medium	Implemented	N/A
2.5 - Cyber Response Playbooks Development	Low	In Progress (Over Due)	Low

Detailed findings

1.1	Significant Assurance	Failure to implement recommended actions from the 2022/23 Information Security Internal Audit report may indicate insufficient commitment or resources dedicated to information security.

Report Ref	Agreed Action	2022/23 Rating	NHS Lothian Reported Progress	IA Evaluation	Current Rating
2.1	**Actions:** We will continue with existing planned and fully funded replacement programmes and document the ongoing risk of national NHS Scotland system non-compliance. Windows XP and Windows 7 will be completely removed from the Estate together with the associated reliance on native MS Access Databases. **Responsible Officer:** Iain Robertson, Head of eHealth Operations and Infrastructure **Due Date:** 31/03/2024	**Medium**	Work is ongoing on removing Windows 7. There are a limited number of devices available, and all remaining devices are logged and the reason for each logged in a register. There are currently 75 machines which are running Windows 7. All are known to eHealth and solutions are being implemented to remove as many of these devices as possible by the March 2024 deadline. The log of remaining devices has been provided to Grant Thornton as evidence. • The green rows have been resolved (13 devices) and will be removed in an update on 19/01/2024. • The orange rows are devices which we have a clear date for replacement with replacement devices arranged with the service (13 devices).	**Implementation is not yet complete.** While the complete removal of Windows 7 is not yet achieved, substantial steps have been taken. Out of the 75 machines running Windows 7, actions for 26 have been identified: 13 resolved and 13 scheduled for replacement. The documentation of remaining devices, along with reasons for their continued use, shows a methodical approach. This level of progress is in line with the March 2024 deadline.	**Low** Risk level reassigned to low, owing to improved mitigation of residual risks.

Detailed findings

1.1	Significant Assurance	Failure to implement recommended actions from the 2022/23 Information Security Internal Audit report may indicate insufficient commitment or resources dedicated to information security.

Report Ref	Agreed Action	2022/23 Rating	NHS Lothian Reported Progress	IA Evaluation	Current Rating
2.2	**Actions:** Revised Azure password policy to be implemented by March 31st, 2023, subject to organisational approval in February 2023. Standard Operating Procedure to be established and implemented by April 30th, 2023. **Responsible Officer:** Iain Robertson, Head of eHealth Operations and Infrastructure **Due Date:** 31/03/2023	**Medium**	The updated Admin & Domain password policy has ensured that all passwords now require to have a minimum of 14 characters, alongside additional complexity enforced by Entra ID. This, alongside the Office 365 multi-factor authentication has addressed the initial action from the report to revise the Azure password policy. The revised Standard Operating Procedure Digital System & Domain Administrator Accounts was approved and released on 10 August 2023. Section 4.5.8 of the Policy has noted that there will be a routine review by NHS Lothian of the policies for each of the systems it manages and to make sure that the password policies for each application are reviewed, considering the latest password policy guidance from NCSC, as required or every 3 years.	**Implementation is complete.** The Admin & Domain password policy has been updated to require a minimum of 14 characters with additional complexity, aligning with NCSC guidelines. Office 365 accounts are now secured with multi-factor authentication. The revised Standard Operating Procedure (SOP), specifically Section 4.5.8, ensures a routine review of password policies, adhering to the latest NCSC guidance. Whilst not implemented in line with agreed dates, this action has now been addressed.	Complete

Detailed findings

1.1	Significant Assurance	Failure to implement recommended actions from the 2022/23 Information Security Internal Audit report may indicate insufficient commitment or resources dedicated to information security.

Report Ref	Agreed Action	2022/23 Rating	NHS Lothian Reported Progress	IA Evaluation	Current Rating
2.3	**Actions:** New password policy to be implemented for Privileged Accounts by 31/03/2023. MFA solution for Privileged Accounts to be deployed by 31/12/2023 **Responsible Officer:** Iain Robertson, Head of eHealth Operations and Infrastructure **Due Date:** 31/12/2023	Medium	The password policy for the above includes all Admin & Domain accounts including Privileged Accounts. A Multi-factor Authentication tool is undergoing the final stages of testing by the Server Team. The current plan is that this will be standard practice for use of Privilege Accounts by April 2024	**Implementation is not yet complete.** The implementation of the new password policy for Admin, Domain, and Privileged Accounts is complete and satisfactory. This part of the audit action is therefore considered fulfilled. However, the deployment of the Multi-factor Authentication (MFA) solution for Privileged Accounts remains in progress. Final testing is underway, with an expected operational date of April 2024. Until the MFA tool is fully implemented and operational, this audit action will remain open and pending completion.	**In Progress - Low** Risk level reassigned to low, owing to improved mitigation of residual risks.

Detailed findings

1.1	Significant Assurance	Failure to implement recommended actions from the 2022/23 Information Security Internal Audit report may indicate insufficient commitment or resources dedicated to information security.

Report Ref	Agreed Action	2022/23 Rating	NHS Lothian Reported Progress	IA Evaluation	Current Rating
2.4	**Actions:** A security phishing exercise will be contracted from a suitable provider, to include senior and administrative staff. **Responsible Officer:** Iain Robertson, Head of eHealth Operations and Infrastructure **Due Date:** 31/08/2023	**Medium**	NHS Lothian contracted a cyber expertise firm for penetration testing after a previous attempt failed due to lack of technical skills. The supplier proposed creating domains for phishing emails to bypass security tools, which eHealth staff approved, excluding content based on the Well Being Campaign. Instead, they used NHS Lothian Parking Survey content. Despite technical adjustments, test emails failed to penetrate, and the suggestion to whitelist the domain was rejected by NHS Scotland. Consequently, the phishing awareness campaign was halted. eHealth continues to caution staff against cyber threats, with recent communications reinforcing awareness of email phishing and malware scams.	**Implementation is complete.** The action, while not executed as initially planned, is deemed complete, but with reservations. The strategy for the phishing exercise proved unfeasible due to technical and administrative barriers. The refusal to whitelist phishing domains by NHS Scotland presents a significant obstacle. As mitigation NHS Lothian has run continuous staff awareness campaigns, including a recent communication on 17/01/2024 to reinforce vigilance against email phishing and malware scams. **Grant Thornton comment** Due to the barriers preventing full implementation as previously agreed by the Committee, there should be consideration of the residual risk held, and appropriate action taken to escalate this if deemed to present a risk which needs further management.	Complete

Detailed findings

1.1	Significant Assurance	Failure to implement recommended actions from the 2022/23 Information Security Internal Audit report may indicate insufficient commitment or resources dedicated to information security.

Report Ref	Agreed Action	2022/23 Rating	NHS Lothian Reported Progress	IA Evaluation	Current Rating
2.5	**Actions:** NHS Lothian will work with a recognised security consultancy organisation to develop a number of cyber response playbooks. **Responsible Officer:** Iain Robertson, Head of eHealth Operations and Infrastructure **Due Date:** 31/08/2023	Low	Consultancy occurred with a cyber security organisation, yielding templates for Playbooks to improve current practices. Staff held workshops with the supplier, obtaining required templates. eHealth collected necessary information, although the process isn't yet fully in playbook format due to time constraints and additional complicating factors. For instance, the first playbook demands specific tools and credentials on a secure laptop, now in place. While playbooks document eHealth's actions, the department reviews, enhances, and records the improved process in the playbook, prolonging the process but ensuring a more efficient outcome. Additionally, Major Incident SOP underwent changes, particularly in communication and incident review, addressing audit points.	**Implementation is not yet complete.** NHS Lothian has consulted with a cybersecurity firm, obtaining templates for cyber response playbooks to improve operational responses. eHealth has compiled the necessary data, but the formalisation of this data into playbooks is still underway and may be delayed due to various complexities. The first playbook requires specific security measures, which have been implemented. To complete implementation, the ongoing process of documenting and formalising eHealth's procedures into playbooks needs to be finalised.	**In Progress - Low** Risk level reassigned to low, owing to improved mitigation of residual risks.

Appendices

Appendix 1:
Staff involved and documents reviewed

Staff involved

- Iain Robertson, Head of eHealth Operations and Infrastructure

Documents reviewed

- Master Windows 7 Spreadsheet
- Domain Password Policy
- Digital System & Domain Administrator Accounts
- Major Incident Report
- Cyber Threat Email

Appendix 2:
Our 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*	Description
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 a number of HIGH rated recommendations)

Appendix 2: Our recommendation ratings

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
Improvement	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

grantthornton.co.uk