NHS Lothian
Internal Audit Report 2022/23
Information Security

Assurance Rating: Moderate Assurance

Date: 08 February 2023

Draft 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
T: 0141 223 0785
E: peter.c.clark@uk.gt.com

Adam Phipps
Manager
T: 0121 387 9069
E: adam.s.phipps@uk.gt.com

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

Timetable

- Date closing meeting held: 5 December 2022
- Date draft report issued: 13 January 2023
- Date management comments received: 27 January 2023
- Date Final report issued: 08 February 2023
- Date presented to Audit and Risk Committee: 20 February 2023

Executive Summary

Introduction

Cybersecurity is the practice of safeguarding systems, networks, programs and data from unauthorised access or criminal use. Cyberattacks typically target one or more aspects of the CIA triad (Confidentiality, Integrity, and Availability). These attacks can be carried out by various types of cyber adversaries, including:

Nation states/Advanced Persistent Threats (APTs): These actors, who are often part of a country's military, target government agencies, critical infrastructure, and industries that contain sensitive data or property. They often use sophisticated methods to disrupt business operations, leak confidential information, and cause significant data and revenue loss.

Organized Crime/Cybercriminals: The main goal of these adversaries is to extort money by stealing or removing access to data or disrupting normal business operations.

Hacktivists: Some groups of cybercriminals are motivated by political or social agendas. They aim to embarrass organisations or publicize damaging information, rather than extort money or assets.

Insider Threats (Malicious or User Error): These threats come from within an organisation and are usually carried out by individuals with authorized access who intentionally or unintentionally compromise the organisation's network, data, or devices. The unique aspect of insider threats is that the access is legitimate. These actors can include current or former employees and third-party contractors.

Script Kiddies: These adversaries, who are not typically technologically sophisticated, exploit specific weaknesses on the internet without fully understanding them. They often discover these weaknesses through others.

Implementing effective cybersecurity measures is becoming increasingly challenging as attackers become more innovative and sophisticated, and there are more devices than people. The review should assess the arrangements in relation to people, processes, and technology.

Scope

Our approach involved interviews with numerous individuals at NHS Lothian, review of supporting documentation and inventory and asset logs to validate the design and operation of the relevant controls in place.

We have applied aspects of the NCSC's 10 Steps to Cyber and reviewed arrangements to meet compliance with this framework and controls in relation to cyber security.

Approach

Our audit approach was as follows:

- Obtain understanding of the key areas outlined in scope above, through discussions with key personnel, review of management information and walkthrough test, where appropriate.
- Identify the key risks relevant within Information Security.
- Evaluate the design of the controls in place to address the key risks.
- Test the operating effectiveness of the controls in place.

It is Management's responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal audit should not be seen as a substitute for Management's responsibilities for the design and operation of these systems.

A complete list of staff involved in the audit and documents reviewed can be seen at Appendix 1.

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.

Cybercrime Threat and Impact

£1.08 million
The average cost of ransomware attacks in the UK

Majority
Of attacks in the social care sector caused by human error

Up to 25%
Losses as a percentage of annual turnover in mid-sized organisations of cyber attacks

197 days
A cyber-attack can take up to 197 days to detect

The public sector, including healthcare organisations like the National Health Service Scotland (NHSS), is a prime target for cybercriminals due to the sensitive and valuable information they hold and their limited resources for cyber defence.

One of the main threats facing the public sector is ransomware attacks. These attacks involve malware that encrypts an organisation's data and demands payment in exchange for the decryption key. Ransomware attacks on healthcare organisations can have severe consequences, such as the disruption of medical services and the loss of patient data. In 2017, the WannaCry ransomware attack affected the UK Health Service, causing widespread disruption and resulting in the cancellation of thousands of appointments and operations.

Another significant threat facing the public sector is phishing attacks. These attacks involve an attacker disguising themselves as a trustworthy entity in order to trick victims into providing sensitive information or transferring money. In the case of the National Health Service Scotland, phishing attacks can lead to the unauthorised access to patient information or the theft of sensitive financial information.

A cyber-attack can take up to 197 days (on average) to detect from the time that the attackers gain access to a network or system. Once an organisation has been targeted, it is more than likely that they will be seen as ‘low hanging’ fruit by cyber attackers, who may return to the business to undertake further exploitation or share knowledge of the organisation’s vulnerabilities with other criminals in dark web forums.

The impact of cybercrime on the public sector can be severe. Ransomware attacks can cause the disruption of essential services and the loss of critical data, while phishing attacks can lead to the unauthorised access to sensitive information and financial losses. In addition to the financial losses, Cyber-attacks on the healthcare sector can have serious consequences on patient care and well-being. Moreover, when it comes to the public sector, the incidents of cyber-attacks can also threaten public trust and confidence in government institutions.

In the case of the NHSS, cybercrime can have a significant impact on patient care and well-being. A ransomware attack on an NHSS organisation can result in the cancellation of appointments and operations, while a phishing attack can lead to the unauthorised access to patient information. The loss of patient data can also result in a violation of privacy and confidentiality.

Summary of Findings

We have concluded that the controls in place in respect of NHS Lothian's Information security provides a **Moderate** level of assurance. The table below 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.

Moderate Assurance			
HIGH	MEDIUM	LOW	ADVISORY
-	4	1	-

Ref	Issue	H	M	L	A
2.1	**Asset management - Unsupported / End of life assets.** NHS Lothian is currently utilising systems and applications that are no longer supported, this poses a significant risk. Without security updates, these assets become increasingly vulnerable to attacks over time and may serve as a point of entry for an attacker. The compromise of these assets could result in short-term loss of business offerings, as well as potential loss of sensitive data or further compromise of NHS Lothian's digital environment. This could ultimately have a negative impact on NHS Lothian's business continuity and disaster recovery operations, as well as the organisations reputation.	-	1	-	-
2.2	**Access Control.** During the audit It was determined that the organisation's current password policy may be insufficient and does not align with best practice guidelines set out by the National Cyber Security Centre (NCSC) or equivalent cyber security frameworks.	-	1	-	-
2.3	**Access Control.** During the audit, it was discovered that there were no controls in place to mandate the use of stronger or more complex passwords for privileged accounts, and no password auditing was conducted to ensure that users were not reusing the same passwords for both privileged and standard user accounts.	-	1	-	-
2.4	**User Engagement - Managing Human Risk.** NHS Lothian currently conducts cyber security awareness training that primarily centres on compliance. Staff receive relevant and current information throughout the year, however, the lack of simulation testing prevents the ability to accurately assess the effectiveness of the training or identify potential weaknesses in human behaviour. As a result, NHS Lothian may not be able to fully establish an effective cyber security culture.	-	1	-	-
2.5	**Incident Response.** During the audit we discovered that NHS Lothian does not currently have cyber security playbooks in place, which raises concerns about the organisation's ability to effectively respond to and manage cyber security incidents. Having well-defined incident response procedures and playbooks is critical for quickly and effectively identifying, containing, and mitigating cyber security incidents, as well as restoring normal operations and reporting the incident to the appropriate parties. The lack of these playbooks leaves the organisation vulnerable to potential cyber security incidents and data breaches.	-	-	1	-
TOTAL		-	4	1	-

Areas of good practice

During the cyber security audit, several areas of good practice were identified. These included strong policies (with the exception of the password policy, see Finding 2.2), regular software updates, and effective incident response procedures. Additionally, NHS Lothian have implemented comprehensive network monitoring solutions that allows them to detect and respond to many potential security threats in real-time. This includes the use of intrusion detection and prevention systems, log management, and regular security reviews of network activity. Overall, the audit revealed NHS Lothian has implemented a number of good practices to protect against cyber threats. The organisation's commitment to maintaining the security of their systems and data is evident in the policies, procedures, and technical controls in place. It is recommended that NHS Lothian continues to review and update its security measures on a regular basis to ensure that they are in line with industry best practices and national standards.

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

Risk area as per scope: Asset Management	
Finding 2.1 – Unsupported / End of life assets.	Medium

Control

Asset management - Unsupported / End of life assets.

Observation

During the audit, it was observed that NHS Lothian was using a number of unsupported or end-of-life assets. These included:

- Outdated operating systems: NHS Lothian was found to be using several versions of operating systems that were no longer supported by their manufacturers. This included Windows XP, which reached end-of-life in April 2014, Windows 7, which reached end-of-life in January 2020, Windows Server 2008 R2, which reached end-of-life in January 2020.
- Unsupported software: NHS Lothian was found to be using software applications that were no longer supported by their manufacturers.

Risk

The use of unsupported systems and applications can have significant consequences for an organisation, as they will no longer receive security updates and will become increasingly vulnerable to attacks. These assets can also be used as a foothold for persistence, allowing attackers to gain access to more systems and sensitive data. Additionally, unsupported assets can disrupt business operations by causing software and hardware to stop working or become incompatible with newer systems.

The compromise of unsupported assets can lead to loss of business and sensitive data, as well as damage to an organisation's digital environment and business continuity. This can ultimately harm the organisation's reputation and ability to recover from a disaster. It is crucial for organisations to regularly assess and replace unsupported assets to mitigate these risks

Recommendation

It is recommended that the corporate management team are aware of the risks of running outdated and unsupported products, and continue to provide support and budget for the Digital team to continue to reduce the risk as much as practicably possible. The appropriate risks associated with these unsupported assets should be recorded on the Digital Department Risk register and reviewed annually. Management may also wish to note that the following steps are being taken by Digital to help further mitigate the risk:

- Prioritise replacement: A plan is already in place which prioritised the client and software replacement with the priority being the client and software which is no longer supported.
- Develop a plan: Note that a plan is in place to deal with these assets, and budget has been made available to create a team dedicated to the update of clients (including out of data software) across NHS Lothian.
- Communicate with stakeholders: Continue to communicate the plan and the need for removing unsupported assets to all relevant stakeholders, including IT staff, management, business units and clinical directorates. The Digital team are also requested to continue to raise these risks and the need to run supported systems in the numerous NHS Scotland Forum where these matters are discussed.
- Implement the plan: Make sure that the programme continues to support the upgrading or replacing unsupported of assets and continues to ensure that all assets are kept up-to-date and that unsupported assets are removed in a timely manner.
- Consider Automation: Note that NHS Lothian have a number of tools in place which automatically detect vulnerabilities or inappropriate network traffic , and that the Digital Team also run monthly scans across the whole estate to identify vulnerabilities on clients and servers for priority remediation.

By following these recommendations, NHS Lothian can effectively remove unsupported assets, reduce the risk of security breaches and technical issues, and ensure that they have the resources they need to operate effectively.

Management Response

Accepted:- The Digital Department will continue to focus on hardware and software replacement to help mitigate the risk. The department has a five-year plan for managing these assets. It should however be noted that the budget which has been identified for this refresh would need to be ring fenced in order to maintain the programme.

Management Action

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.

Responsibility: Head of Digital Operations	Target Date: 31/03/2024

Risk area as per scope: Access Control & Identity and Access Management

Finding 2.2 – Potentially Insufficient Access Controls	Medium

Control

Access control & identity and access management (IAM) and password management control includes all the procedures and policies that an organisation puts in place to ensure the secure creation, storage, and management of passwords. This includes guidelines for creating strong passwords, implementing multi-factor authentication, and regularly changing passwords. It also includes procedures for securely storing passwords, such as using password managers or encryption, and monitoring for suspicious activity.

Observation

During the audit, it was determined that the organisation's current password policy may be insufficient and does not align with guidelines from the National Cyber Security Centre (NCSC) or equivalent cyber security framework.

Risk

Potentially insufficient password policies can have a significant impact on the organisation's security. Weak or easily guessable passwords can be easily compromised, leading to unauthorised access to the organisation's systems and data. Reusing passwords across different accounts increases the risk of a password being compromised, as a single compromise can lead to multiple breaches. The lack of regular password audits can also lead to the use of outdated or weak passwords. Examples of commonly known weak passwords that conform to NHS Lothians current password policy (at least 8 characters, including one lowercase letter, one uppercase letter, and one special character) are listed in the table below:

P@ssword1	P@ssw0rd1	Zxcvbnm1@	12345678A#
Abcdefgh1@	Welcome1@	Liverp00l1	Zxcvbnm1@
QwertyuI@	Welcome2@	Qwerty!23	12345678A@
AsdfghjK1	Welcome3@	Welcome4@	123456789A@

It's important to note that even though these passwords meet the complexity requirements of an 8 characters, one lowercase, one uppercase and one special character, they are considered bad passwords because they are commonly used and easily guessable. Therefore, it's recommended to use unique and complex passwords that are not easily guessable, and not to use the same password across different accounts. Additionally, organisations can also use measures such as multi-factor authentication and controls to prevent the use of known bad passwords to further increase security.

Recommendation

To ensure the security of passwords and align it to guidelines from the National Cyber Security Centre (NCSC), Management may wish to consider implementing the following recommendations:

- Passwords should be a minimum of 12 characters in length.
- Passwords should not contain easily guessable information such as the user's name or date of birth.
- Passwords should be complex, including a mix of uppercase and lowercase letters, numbers, and special characters.
- Measures should be put in place to prevent the use of known bad passwords.
- Users should not use the same password for multiple accounts.
- Passwords should be regularly reviewed and updated.
- organisations can consider using a password manager to securely generate and store strong passwords.

The overall goal is to ensure the passwords are strong and unique, and not easily guessable by potential attackers. This is done by implementing measures to prevent the use of known bad passwords, increasing the length of passwords, and adding complexity to the password. It is also important to regularly check and update passwords, and not to use the same password across different accounts.

Management Response

Accepted. NHS Lothian have identified that the Azure Password requires to be revised, with the length to be increased to 14 in line with colleague organisations, including activating complexity and weak password requirements. Other systems that are technically capable are already in compliance. NHS Lothian will develop and implement a new Standard Operating Procedure to review passwords on a 24 month basis to check the password configuration of each system managed by the department.

Management Action

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.

Responsibility: Head of Digital Operations	**Target Date: 30/04/2023**

Risk area as per scope: Access Control	
Finding 2.3 – Potentially Insufficient Access Controls (Privileged User Account)	Medium

Control

Access Control & Identity and Access Management (IAM) Password management control includes all the procedures and policies that an organisation puts in place to ensure the secure creation, storage, and management of passwords. This includes guidelines for creating strong passwords, implementing multi-factor authentication, and regularly changing passwords. It also includes procedures for securely storing passwords, such as using password managers or encryption, and monitoring for suspicious activity

Observation

During an audit of NHS Lothian's network security controls, it was discovered that there were no controls in place to mandate the use of stronger or more complex passwords for privileged accounts. Additionally, no password auditing was conducted to ensure that users were not reusing the same passwords for both privileged and standard user accounts. This presents a significant security risk to NHS Lothian, as privileged accounts are a prime target for attackers.

Risk

The lack of controls for privileged account passwords presents a significant risk to NHS Lothian. Without stronger or more complex passwords, privileged accounts are more vulnerable to brute force attacks and dictionary attacks. Additionally, the lack of password auditing means that users may be reusing the same passwords for both privileged and standard user accounts, increasing the risk of unauthorised access.

Recommendation

Currently NHS Lothian privileged user accounts are unique for each user, separate from business accounts and have account lockout. Logging in from a NON-NHS endpoint requires MFA.

However, in order to mitigate the risk of unauthorised access and data breaches, it is recommended that NHS Lothian implement the following controls for privileged account passwords:

- Implement a password policy that requires stronger or more complex passwords for privileged accounts, including minimum length - Passwords should have a minimum length of at least 20 characters to ensure they are difficult to guess or crack and use complexity, Passwords should include a combination of uppercase and lowercase letters, numbers, and special characters to increase their complexity.
- Unique: Passwords should be unique to each privileged user account and should not be used for other accounts or systems.
- Protection against automated attacks: The use of password cracking software and automated scripts can be mitigated by using mechanisms like rate-limiting or account lockout.
- Conduct regular password audits to ensure that users are not reusing the same passwords for both privileged and standard user accounts.
- Consider implementing multi-factor authentication for privileged accounts to provide an additional layer of security.
- Provide employee training on good password hygiene to help ensure that users are aware of the importance of strong and unique passwords.

Management Response

It is noted that currently NHS Lothian privileged user accounts are unique for each user, separate from business accounts and have account lockout. Logging in from a NON NHS endpoint requires MFA.

Also implementation of the improvements to the Azure Password as indicated in item 2.2 above, will provide a number of additional security measures identified, including activating complexity and weak password requirements. The tools being deployed prevent reusing of passwords for all accounts.

NHS Lothian will deploy MFA for all privileged accounts . We are not aware of tools which would allow comparison of accounts as suggested, and would be concerned if such tools existed that they could readily be exploited by hackers. Management believe deploying MFA for these accounts is recognised best practice for such accounts.

Management Action

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

Responsibility: Head of Digital Operations	Target Date: 31/12/2023

Risk area as per scope: Access Control	
Finding 2.4 – User Engagement - Managing Human Risk.	Medium

Control

Phishing is a type of social engineering attack that typically comes under the category of "Access Control" in the broader field of Cybersecurity. Access control is a security technique that regulates who or what can access and use a system, network, or resource. The main purpose of access control is to ensure that only authorized individuals or systems can access sensitive information or perform critical functions.

Phishing attacks often involve tricking users into revealing sensitive information, such as login credentials, or into visiting a malicious website. It involves sending malicious e-mails, text messages or social media messages that appears to come from a trustworthy source like financial institution, a colleague or a friend. Therefore, anti-phishing measures like anti-phishing software, employee training, and simulated phishing tests all come under Access Control. These controls are used to protect the company's sensitive information and reduce the risk of falling for a phishing attack.

Observation

NHS Lothian conducts cyber security awareness training for staff, which places emphasis on compliance. Staff receive useful and current information on a regular basis, however, the lack of simulated testing makes it impossible to evaluate the efficacy of the training or pinpoint any vulnerabilities in human behaviour. This hinders the ability to establish a strong cyber security culture throughout NHS Lothian .

Risk

Individuals have emerged as the primary target for cyber criminals globally, making them a major threat to organisations. Security awareness programs, along with the professionals who handle them, play a vital role in addressing this human risk. Currently, NHS Lothian has not been able to successfully conduct phishing tests due to all attempts being successfully blocked by Firewalls and other security controls. Some of the main risks that can be highlighted by phishing tests include:

- Lack of awareness: Without simulated phishing exercises, staff may not be aware of the different types of phishing emails or messages they may encounter, making them more vulnerable to falling for a real phishing attack.
- Inability to detect phishing attempts: Without regular simulated phishing exercises, staff may not be able to detect real phishing attempts, which can lead to the compromise of sensitive information.
- Difficulty in assessing staff's susceptibility: Without simulated phishing exercises, it may be difficult for management to assess staff's susceptibility to phishing attempts, making it difficult to identify and address vulnerabilities.
- Difficulty in measuring the effectiveness of training: Without simulated phishing exercises, it can be difficult for management to measure the effectiveness of their cyber security training, making it difficult to identify areas for improvement.
- Lack of preparedness: Without simulated phishing exercises, staff may not be prepared to handle real phishing attempts, which can lead to costly data breaches or other security incidents.

Overall, simulated phishing exercises are important for identifying vulnerabilities, assessing staff's susceptibility to phishing attempts and measuring the effectiveness of training. It's important to perform regular simulated phishing exercises to increase staff's awareness and preparedness to handle phishing attempts.

Recommendation

NHS Lothian already promotes a security culture that emphasises that cyber security is not just an IT concern but an organisational safety concern. All staff must complete a mandatory training module on Cyber Security and Information Governance in addition to regular awareness sessions being run across the organisation.

Management should consider implementing regular phishing simulation campaigns to test efficacy of the forementioned training, in addition to testing staff awareness and their susceptibility to providing information to cybercriminals through spoofed emails and other types of messages. This should be done on a monthly basis. Overall, the goal is to improve staff training and awareness of the implications of cyber-attacks and what can be done to mitigate the risk.

Management Response

Previous phishing exercise (contracted from a security company) failed as Lothian firewalls and other controls blocked the attempts to reach users. It is agreed that another phishing exercise to be contracted but this to only include senior and administrative staff. The risk of disruption to clinical staff performing clinical duties is deemed as a risk and another approach to be planned.

Management Action

A security phishing exercise will be contracted from a suitable provider, to include senior and administrative staff

Responsibility: Head of Digital Operations	Target Date: 30/08/2023

Risk area as per scope: Incident Response	
Finding 2.5 – limited number of cyber playbooks	Low

Control

Incident response

Observation

It was noted that while there are extensive plans for business continuity and disaster recovery, there are only a limited number of cyber playbooks available for first responders in the event of a cyber-attack. Furthermore, there is a lack of comprehensive simulation or live testing for a wide range of potential events, such as cloud based attacks, ransomware/malware attacks, insider threats, data loss or exposure, network intrusion, DDoS, and phishing.

Risk

Cybersecurity threats are becoming increasingly prevalent and sophisticated, making it crucial for organisations to have a plan in place for responding to potential incidents. A cyber incident response plan, also known as a "playbook," is a document that outlines the steps an organisation should take in the event of a cyber attack or data breach. Without a written incident response plan, organisations are at risk of not being able to respond quickly and effectively to a cyber incident, potentially leading to significant harm. Risks of not having a written incident response plan:

- Lack of preparedness: Without a clear incident response plan in place, organisations are more likely to be caught off guard when a cyber incident occurs. This can result in a delay in responding to the incident, which can make it more difficult to contain the damage and recover from the attack.
- Inability to coordinate responses: A written incident response plan allows all members of an organisation to understand their role in responding to a cyber incident. Without a plan, there is a risk of confusion and lack of coordination among employees, which can make it more difficult to respond to the incident effectively.
- Lack of standard procedures: Without a written incident response plan, organisations may not have standard procedures in place for responding to a cyber incident. This can lead to inconsistent responses and a lack of clear direction on how to proceed.
- Difficulty in communicating with stakeholders: A written incident response plan can help an organisation communicate effectively with stakeholders, including customers and regulatory bodies. Without a plan, an organisation may struggle to communicate effectively, which can lead to mistrust and damage to the organisation's reputation.

Recommendation

It is recommended that the organisation establish a cross-functional incident response team responsible for the development, testing, and maintenance of incident response playbooks. The playbooks should be reviewed and updated on a regular basis to ensure they align with the organisation's current threats and risks. The incident response playbooks should include, but not limited to:

- Identification of the incident, including the scope and impact
- Initial response procedures and contact information for the incident response team
- Steps for containing and mitigating the incident
- Procedures for preserving evidence
- Communication plan and procedures for internal and external stakeholders
- Post-incident recovery and restoration procedures
- Procedures for reviewing and learning from the incident

The incident response team should conduct regular tabletop exercises to test and validate the playbooks and should also conduct regular training for all employees to familiarise them with the procedures outlined in the playbooks. Having a written incident response plan is critical for organisations to be able to respond quickly and effectively to a cyber incident. It's recommended that the organisation creates and implements incident response playbooks to minimize the risks and damages caused by cyber incidents.

Management Response

Partially Accepted:- It is noted that in Lothian there are already extensive plans for business continuity and disaster recovery.

NCSC Exercise in a Box simulation exercise has been successfully completed by Lothian with lessons learned, but it is agreed that “Playbooks” to be investigated and put in place.

Management Action

NHS Lothian will work with a recognised security consultancy organisation develop a number of cyber response playbooks.

Responsibility: Head of Digital Operations	Target Date: 31/08/2023

Appendices

Appendix 1 – Staff Involved and Documents Reviewed

Staff Involved

- Information Governance and Security Manager
- IT Security Manager
- Technical Services Manager
- Customer Service Manager, eHealth
- Head of eHealth Operations and Infrastructure

Documents Reviewed

- NISR - 2022 Review Report - Lothian.pdf
- Remote access to Servers from Suppliers SOP 2021.docx
- Desktop and Server Operating System Patching SOP v.2.docx
- Digital System & Domain Administrator Accounts SOP v1.05 - 2022 IN DEVELOPMENT.docx
- Vulnerability Scanning SOP 2021.docx
- Threat Detection SOP 2022.docx
- Device Management SOP v.2.1 2021.docx
- Change Management SOP 2022.docx
- Health - Technical Services Policy 014 System access and password management SOP.pdf
- Access to Applications and Network Policy.docx
- Digital Operations Leavers - System Access Removal SOP 2019.docx
- Backup Schedule Amendment SOP 2022.docx
- System Logs SOP v6 - 2022 IN DEVELOPMENT.docx
- NHSL Digital IT Security Policy.docx
- NHS Lothian Home Working Policy 1.0.doc
- Working from Home IG Policy Statement 04092020.docx
- Data Protection Policy.docx
- Data Protection Impact Assessment Guidance Final.rtf
- Firewall SOP 2019.docx
- Reference - FIREWALL SOP - Firewall Default Denies.docx
- Corporate Risk Register Cyber Security Risk 01032022.docx
- Risk Mitigation Plan for Corporate Risks - Cyber Security May 2022.docx
- IT Department Risks Nov 2022.xlsx
- IG Highlight Report Oct 22.docx
- Digital Major Incident Plan v4.doc
- Resilience Assurance Protocol 2021-2022.pdf
- Digital Service Continuity 2022.docm
- Assurance pro forma - Digital Plans & T&E 2022 v.2 with Telecoms.docx
- EXAMPLE TRAK Resilience Plan 2022.docx
- EXAMPLE HEPMA Resilience Plan 2022.doc
- Major Incident SOP 2022.docx
- Resilience SOP 2022.docx
- M365 Quick Sheet - Sensitivity Labels V1.1.pdf
- Information Risk Management Policy.docx
- Information Security Mgt System (ISMS) Policy.docx
- Data Access Policy.docx
- Data Access for Research Policy.docx

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 3 - 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

grantthornton.co.uk