THE CHIEF CONSTABLE OF CLEVELAND

Cyber Security Review

Internal audit report 3.22/23

FINAL

12 August 2022

1. EXECUTIVE SUMMARY

Why we completed this audit

As part of the approved internal audit plan for 2022 / 2023, we have undertaken a review of cyber security at the Force. This review focussed on the areas of risk management, incident management, logging and monitoring, asset management, and data security.

IT at the Force is governed by the Head of ICT, who is supported by the Head of ICT Service and Operations and the Head of ICT Programme Delivery. Service and operations oversees branches covering: infrastructure (infrastructure and network), radio and mobile, GIS, applications, support, and service management. Logging and monitoring activities are primarily outsourced to the National Management Centre (NMC), which is part of the Police Digital Service national institution, who develop capabilities and ways of working that enable police services to adapt to and deal with the complexity of a rapidly changing technological world.

Since the onset of the COVID-19 pandemic, increases in cyber-attacks and threats have been reported by a number of organisations internationally, such as the NCSC (National Cyber Security Centre). Organisations, such as the Force, who hold large quantities of sensitive and confidential data are at risk for cyber-crime. As such, a robust control environment over key areas of the IT landscape is vital to avoid regulatory sanctions alongside financial and reputational damages.

Conclusion

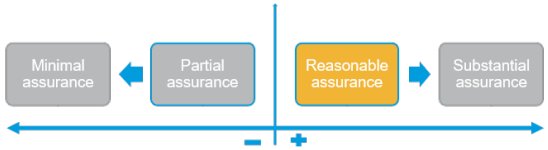
During our review, we noted two instances of controls which were not designed or operating adequately, with the remaining controls working correctly and effectively mitigating risks. Overall, we noted that the Force have adequate risk and incident management controls in place, alongside effective logging and monitoring supported by NMC threat intelligence alerts.

While effective physical asset management processes are in place, work is still being undertaken to populate the Information Asset Register (IAR). We identified during the review that this register currently lacks criticality scorings for entries, which would allow management to enhance the effectiveness of responses to breaches or loss of information assets.

It was also found that the network passwords configured were weaker than the requirements documented in the Force's policy and were insufficiently robust given the nature of the organisation and data held. As such, we have raised **one high** and **one medium** priority management actions.

Internal audit opinion:

Taking account of the issues identified, the Chief Constable of Cleveland can take **reasonable assurance** that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective.



However, we have identified issues that need to be addressed in order to ensure that the control framework is effective in managing the identified risk.

Key findings

We identified the following findings that have resulted one high and one medium priority management actions being raised:

Review of the network password configuration within Active Directory (AD) Group Policy found that the parameters set were not in-line with the requirements documented for users within the policy. Furthermore, the length and robustness of the configuration was below that recommended by reputable independent bodies such as the National Cyber Security Centre (NCSC), and was insufficiently secure given the nature of the organisation and data held within systems. **(High)**

Work is currently underway on the Information Asset Register, held within SharePoint, with audits undertaken to identify information assets held by the Force alongside their applicable owners. However, review of the IAR, corroborated by enquiry with the GDPR Officer, found that criticality of data is not currently recorded for information assets. **(Medium)**

Our audit review identified that the following controls are suitably designed, consistently applied, and are operating effectively:

A Corporate Risk Register is maintained on the 4Risk risk management application. This contains overarching, broad "big ticket" IT concerns (based on previous incidents and other incidents experienced by organisations in the sector) and is reviewed on a quarterly basis. A small number of other risks are populated onto the register if they reach the predetermined threshold.

A separate Information Security Management System (ISMS) Risk Register is in place, sourced from previous incidents, business processes reviews, and GDPR preparation/reviews. In addition, the Head of IT Service and Operations maintains a 'hit list' of cyber risks and issues documented in a Monthly ICT Service Delivery Report, which typically consist of software or infrastructure to be patched in order to remediate an identified vulnerability.

The ‘POLWARP’ email inbox is used by IT staff to monitor email feeds of threat intelligence from external sources. These include Threat Landscape Summary emails from the NMC; emails show a read status, indicating IT staff are actively reviewing the mailbox. In addition to this, the Head of IT Service and Operations and team monitor feeds of vendor information (e.g., Cisco updates) for awareness of new threats, and staff monitor media (including social media) for upcoming vulnerabilities.

Monitoring for potential threats is performed via a combination of automated alerts and outsourced monitoring, with procedures in place to respond to incidents and report to the Home Office.

A documented Information Security Incident Response Plan is in place, as well as an Information Security Policy. Per this documentation, incidents must be reported within 24 hours to a supervisor. Escalation to an incident may also take place from patterns noticed by the service desk team. On a daily basis, the Information Security Manager will check for new incidents, including examining the InfoSec mailbox for general alerts. On a quarterly basis, IT will provide a spreadsheet of incident tickets (including near misses) to the Home Office. Logging and monitoring are primarily outsourced to the NMC, utilising the NMC's Security Information and Events Management (SIEM) tool. Feedback and results from the NMC take the form of daily emails and weekly round-up emails sent to specific email distribution lists. Internally, there is a Microsoft System Center Configuration Manager (SCCM) Infrastructure feed which delivers to a MalwareAlert inbox/mailing list. While most malware alerts are automatically quarantined and managed by the anti-malware solution, they will be escalated if judged by IT personnel to be serious enough for an incident, such as a series of repeat alerts.

No exceptions were identified from sample testing of incidents or of the logging and monitoring in place.

Physical assets are recorded and reviewed in accordance with documented policies and procedures.

Policies around physical asset management are documented within the Asset Management Process Working Instructions and a separate Asset Management Policy. At the time of the audit, there were plans in place to combine this into a single formal Asset Management Policy/Procedure document in the near future.

At present, separate repositories are used for different types of physical assets due to the diverse types of management required. However, the Force are currently in the process of implementing an add-on to the existing Cireson System Center Service Management (SCSM) solution to combine these into a single service management solution and physical asset register. This will centralise all information on physical assets, such as criticality ratings for devices and maintenance schedules. As part of this project, the SCCM feed will be imported first, followed by the remaining asset repositories.

Firewalls are managed in-house, with a contract in place with third-party Pentesec for support over the check point firewall. Firewalls are configured using a default deny policy, which is considered best practice. Changes to firewall rules are made by the Network team, and requests are submitted via two routes:

1. A request from a user may be sent via Cireson, typically for access to a specific blocked URL. In these instances, approval is sought from the Information Management team and, upon receipt of this, the firewall rule is added by the Network team.

2. A request may come internally from within the IT team, typically from system administrators/software services. For these requests, a form is completed by the requestor, which requires their line manager approval. This process is mapped internally within the Cireson system.

No exceptions were identified from sample testing of firewall changes, and comparisons of the users authorised to make such changes to an organisational chart found that all such staff were appropriate.

Encryption of externally transferred data is managed and configured by the NMC. Internally, several encryption methods are used, including: protocol and cipher-based encryption for internal data transfer and VPN traffic, Wi-Fi Protected Access 2 (WPA2) Enterprise AES on the Police Wi-Fi network, and Bitlocker encryption on device hard drives. Ivanti is used to manage external data devices (e.g. USB) and to encrypt external data devices and restrict access to specific users with a separate password. Backup tapes are encrypted automatically via the NetBackup Key Management Service, which manages symmetric cryptography keys for the tape drives that conform to the T10 standard.

NetBackup is used to manage backups. Backups are stored across two types of appliances: NetBackup 5240 and 5250 immutable storage devices. Encrypted recovery points are replicated between both the Disaster Recovery (DR) site and primary site to encrypted tape, which is then housed on-site.

Inspection of the backup configuration confirmed that file servers have a retention period configured of one year for monthly backups and five weeks for daily backups across both the main and DR sites. VM servers have a retention period of five weeks across both sites. Full backups for file servers are taken both daily and monthly, with the monthly backup having assigned storage under ‘SLP_HQ_Monthly’. VM servers have full backups daily.

For a sample of dates, we inspected the backup log and noted that backups had been completed successfully, with any failures investigated and followed by subsequent successful backups. We inspected the report of restores for the past year and noted that successful restores had taken place consistently multiple times a month over the past 12 months.

Multi-Factor Authentication is enabled on Microsoft 365 as part of the agreement with the NMC. This reduces the risk of unauthorised access to systems and data in the event that logon credentials are compromised.

2. DETAILED FINDINGS AND ACTIONS

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Risk Reference: 1685			
Control	A documented password policy is in place, included within the passwords procedure document (Passwords Standard Operating Procedure v1.0). General user passwords must be at least 10 characters long and must contain at least three of the following: • Lower case letters; • Upper case letters; • Numeric digits; and • Symbols. General user passwords may be user selected or provided by a generator on the information security internal site. Privileged account passwords must be chosen from those offered by the admin password generator on the Information Security site.	**Assessment:** **Design** ✓ **Compliance** ×	
Findings / Implications	We inspected the Active Directory (AD) Group Policy password configuration for the Force domain, and noted that the following rules were configured: • Password history of eight passwords; • Maximum password age of 90 days; • Minimum password length eight characters; • Complexity requirements enabled; and • Account lockout for 30 minutes after five invalid attempts. The current password set up is not in-line with the organisational policy documented in the Passwords Standard Operating Procedure, and below the standards expected for secure passwords in particular given the highly confidential and sensitive data and systems in use at the Force. The National Cyber Security Centre (NCSC) guidance advises organisations to:		

Risk Reference: 1685

- Not enforce regular password expiry of 30/60/90 days and instead use a longer expiry period;
- Avoid complexity requirements that encourage users to make common substitutions (e.g. swapping ‘o’ to ‘0’);
- Avoid using any maximum length requirements that a user might try to exceed, as they will make it harder for users to choose a suitable password that fits the length criteria.
- Password length should only be capped by the capabilities of the system; and
- Implement and promote awareness of the ‘three random words’ technique to generate longer passphrases that are more resistant to common password exploitation techniques.

The above should be used in combination to avoid the creation of weak points in the password control.

In addition, it was found that no separate, more stringent requirements are logically enforced for privileged accounts.

Inspection of a separate password rationale document (‘Passwords Security Operating Procedure – Rationale’) showed that management at the Force are already aware of the weakness of this password setup. This document noted that:

"A significant proportion of passwords were cracked during penetration testing in mid-2020. This suggests too many passwords are weak. The report states

> *In total 8,500 passwords were extracted from the Domain Controller, out of these:*
>
> - *2763 (32.5%) of the passwords could be cracked using a dictionary-based wordlist*
> - *124 (~4%) of the passwords cracked were a variant of the word ‘password’*
> - *694 (25%) of the passwords cracked were of 10 characters in length.*

Some of those passwords cracked belonged to administrators. Breaches of such accounts are more serious."

Two options were recommended within this document, both of which are appropriate sets of parameters which management could action:

- *" A moderate increase in password length is appropriate for the general user population targeting a lower threshold of 45 bits of entropy. Due to the risks associated with admin users, a substantial increase with machine-generated complexity of c. 80 bits is appropriate. This can be achieved by six lower case letters, two upper case letters, two digits and two symbols (drawn from 25) (total is 77.3 bits of entropy).”*
- *“Other work around usability advocates passphrases, as does NCSC (see earlier). Choosing three random words from a list of 1296 words, plus a digit, a symbol and forcing some of the initial letters of the words to be capitals gives around 40 bits of entropy. A longer version with four words, etc. gives over 50 bits."*

Risk Reference: 1685				
	We therefore note that, while the Force recognise the need for changes to currently configured password policies to increase robustness, the current configuration enforced does not meet recommended guidance and is not appropriate for the nature and sensitivity of the systems and data it protects. In addition, user guidance is different to that is logically enforced, which may create confusion amongst staff. Without robust password parameters logically configured, there is an increased risk of unauthorised access to systems and data, potentially leading to data theft or loss, or the facilitation of criminal activities.			
Management Action 1	Management will reconfigure existing logical password configurations to meet current best practice guidance and increase robustness. It is recommended that reputable external guidance (such as that issued by the NCSC) is used as a baseline for this. In addition, management will logically enforce stronger password requirements for privileged accounts.	**Responsible Owner:** Information Security Manager	**Date:** 31 August 2022	**Priority:** **High**

Risk Reference: 1685			
Missing Control	**Missing control** The Force follow the Information Commissioner's Office (ICO) structure for handling information assets, with a Senior Information Risk Owner (SIRO) in place (currently the Deputy Chief Constable) and Asset Owners in place. A complete and accurate Information Asset Register (IAR) is maintained centrally in SharePoint. The IAR also tracks data protection audits completed to identify and capture data on information assets.	**Assessment:** **Design** **Compliance**	 × -
Findings / Implications	The IAR is currently incomplete, with core information missing for some entries such as Data Protection Impact Assessments (DPIAs) for some systems which store personal data. The IAR is hosted within SharePoint, and also contains a record of internal data protection audits carried out, which capture all audit information gathered. 79 audits in total have been recorded within the IAR at the time of this review. Of these: • 56 are complete; • Seven are duplicates; • Three are in progress; and • 13 are awaiting further information now they are completed. We were informed, however, that a new role has been secured for an Information Governance Manager. A core responsibility of this role will be to deal with gaps identified in the IAR once in place, in particular gaps in DPIAs. Inspection of the Information Asset Register (IAR) identified that there is no system in place at present for determining the criticality of information assets for ICO/General Data Protection Regulation (GDPR). While a 'Category 1' list of priority for systems is documented within the ICT Disaster Recovery Plan, this information does not fully map to information assets and does not consider risks and impacts from a GDPR/UK Data Protection Act perspective when allocating its rating. Additionally, the priority ratings from the ICT Disaster Recovery Plan have not been incorporated into the IAR and fall under separate ownership within the organisation. Without appropriate documentation of the criticality of each information asset, there is an increased risk that information assets are not assigned appropriate priority or weighting during IT incidents or in the event of a data breach or loss. In addition, there is an increased risk that the criticality of information assets from a data protection perspective is not aligned to the criticality scorings assigned to such assets and systems within disaster recovery and business continuity procedures.		

Risk Reference: 1685				
Management Action 2	Management will continue the exercise of allocating DPIAs and filling gaps and missing fields within the IAR. As part of this, management will include a rating on the criticality of each information asset (considering both the criticality of the asset to business operations and the criticality of the asset from a data protection perspective).	**Responsible Owner:** GDPR Auditor	**Date:** 31 Aug 2023	**Priority:** Medium

APPENDIX A: CATEGORISATION OF FINDINGS

Categorisation of internal audit findings	
Priority	**Definition**
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

The following table highlights the number and categories of management actions made as a result of this audit.

Risk	Control design not effective*		Non-Compliance with controls*		Agreed actions		
					Low	Medium	High
Risk Reference: 1685	1	(17)	1	(16)	0	1	1
Total					**0**	**1**	**1**

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

APPENDIX B: SCOPE

The scope below is a copy of the original document issued.

Scope of the review

The scope was planned to provide assurance on the controls and mitigations in place relating to the following risk:

Objective of the review	Risk relevant to the scope of the review	Risk source
To provide assurance that computer systems and data are resilient to threats resulting from their connection to the Internet.	Risk Reference: 1685	Risk register

The following areas will be considered as part of the review:

The remit of the review will include an evaluation of five of the ten control areas that have been identified by the National Cyber Security Centre (NCSC) of UK Government as key control areas for cyber risk management. These have been chosen based upon the key concerns and strategic objectives expressed by management, and are:

Risk management

An assessment of the high-level controls focussing on:

- Suitability of current IT security risk management processes and procedures.
- Risk assessments or business wide cyber exposure assessments.
- Procedures relating to risk identification.
- Senior management oversight of and responsibility for Cyber risks.

Asset management

An assessment of the high-level controls focussing on:

- Processes for identification of assets both physical and logical.
- Criticality identification of assets and the data stored.
- Asset register of identified assets.

Data security

An assessment of the high-level controls focussing on:

- Firewall rules, network access controls and settings.
- Password policy and authentication controls and exceptions.
- Encryption technology employed for in transit, in processing and at rest.
- Backup policies, procedures, and tools.
- Restore testing procedures.

Incident management

An assessment of the high-level controls focussing on:

- Incident management and incident response policies and procedures.
- Past incident management records.
- Lessons learned and root cause analysis records.

Logging and monitoring

An assessment of the high-level controls focussing on:

- Logging and monitoring technologies.
- Dashboards and alert identification for logs and monitoring events.

The following limitations apply to the scope of our work:

- The scope of our work will be limited only to those areas that have been examined and reported and is not to be considered as a comprehensive review of all aspects of cyber security risk.
- The approach taken for this review will be to validate the design of controls and testing of key controls.
- We will be testing key controls on a sample basis and for the financial year 2021 and year to date 2022 only.
- We will not perform penetration tests and vulnerability assessments however we will review the results of tests undertaken by independent service providers.
- The information provided in the final report should not be considered to detail all errors or risks that may currently or in the future exist within the network infrastructure environment, and it will be necessary for management to consider the results and make their own judgement on the risks affecting the organisation and the level of specialist computer audit coverage they require in order to provide assurance that these risks are minimised.
- In addition, our work does not provide an absolute assurance that material error; loss or fraud does not exist.

Debrief held	20 July 2022	**Internal audit Contacts**	Daniel Harris, Head of Internal Audit
Draft report issued	8 August 2022		Philip Church, Senior Manager
Responses received	12 August 2022		Michael Gibson, Manager
			Paul O'Leary, Technology Risk Assurance (TRA) Lead
			Rich Dillon, Technology Risk Assurance Associate Lead
			Charley Mather, Technology Risk Assurance Senior Consultant
Final report issued	12 August 2022	**Client sponsor**	Head of ICT
		Distribution	Head of ICT

rsmuk.com