THE CHIEF CONSTABLE OF CLEVELAND

Select Key IT Security Controls

Internal audit report 14.23/24

FINAL

21 June 2024

This report is solely for the use of the persons to whom it is addressed. To the fullest extent permitted by law, RSM UK Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party.

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

1. EXECUTIVE SUMMARY

Why we completed this audit and background

As part of the approved annual 2023/24 Internal Audit plan, we conducted an audit of Select Key IT Security Controls. The objective of this audit was to evaluate the design of key cybersecurity controls in place and assess the operating effectiveness of selected controls from the Security Assessment for Policing (SyAP) control framework that is based on the NIST (US National Institute of Standards and Technology) cybersecurity framework. This encompassed controls from each of the five key areas: Identify, Protect, Detect, Respond, and Recover. By conducting this audit, we aimed to provide insights into the Force's cybersecurity posture, identify areas for improvement, and agree actionable measures to enhance the overall security resilience.

Weaknesses in an information security framework can lead to various security vulnerabilities, including unauthorised access to sensitive data, systems, or resources, data breaches, insider threats, malware infections, and service disruptions. These vulnerabilities can result in severe consequences such as financial losses, reputational damage, regulatory non-compliance, legal liabilities, and loss of public trust.

The audit was carried out primarily through meetings with key information security and ICT staff remotely, along with an assessment of key documentation relevant to the scope of the audit.

Conclusion

Our assessment identified several areas for improvement within the Force’s information security framework that require management attention. These include opportunities to enhance vulnerability tracking, establish documented processes for managing third-party access, standardise vulnerability scanning practices, and improve user education and awareness efforts. Addressing these areas is vital for enhancing the Force's resilience to potential security incidents and safeguarding its IT systems and data integrity.

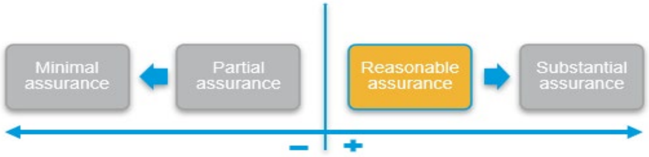
While these areas for improvement indicate a need to strengthen Force's security practices, it is important to recognise the areas where controls are adequately designed and operational. The Force has well designed controls in place regarding software asset management, access permissions, network architecture, backups, event data monitoring, antivirus protection and incident management, demonstrating a commitment to implementing robust security measures and maintaining resilience against cybersecurity threats.

Moving forward, the Force must prioritise addressing the identified weaknesses while leveraging and enhancing its existing strengths. By taking proactive steps to strengthen its security posture and continuously improving its security practices, the Force can mitigate risks effectively and ensure the protection of its critical assets against evolving cybersecurity threats.

Internal audit opinion:

Taking account of the issues identified, the Chief Constable of Cleveland can take **reasonable assurance** that the controls upon which the Force rely 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 weaknesses for which we agreed four medium and three low priority actions (please find the low priority findings documented within the detailed findings section below):

Vulnerability Tracking

The Force conducts an annual penetration test, documenting actions in a tracker. Although management have stated that efforts to address issues have been implemented, the tracker's status column lacks completion, risking unaddressed vulnerabilities. This could invite exploitation by threat actors, posing security risks such as data breaches. Previously, a ticketing system tracked vulnerabilities, but now only significant threats are ticketed, hindering tracking for lower-level issues. Without centralised tracking, accountability for addressing these vulnerabilities is compromised, potentially leading to delays or oversights in mitigation efforts. **(Medium, MA1)**

Third-Party Access Control

Processes for third party access control have not been documented. Without documented processes for managing third-party access, there is a higher risk of security vulnerabilities. Third parties may gain unauthorised access to sensitive systems, data, or resources, leading to data breaches, unauthorised disclosures, or other security incidents. **(Medium, MA2)**

Vulnerability Scanning Processes

Information pertaining to vulnerability scanning has not been included within the ICT Infrastructure Information Security Expectations document. Without documented processes, vulnerability scanning activities may be inconsistent or inefficiently executed. This can result in missed vulnerabilities, incomplete scans, or inaccuracies in the assessment of the Force's security posture, leaving critical systems and data exposed to potential exploitation. **(Medium, MA3)**

User Education and Awareness

The Force offers a robust information security training program featuring two mandatory courses. Training progress is monitored through an e-learning Power BI system. Analysis of the Power BI dashboard identified a 77% completion rate for the managing information: Operational course and a 54.6% completion rate for managing information: Non-Operational for users that have completed the training of the past two years (on a rolling basis). Employees who fail to grasp data protection concepts are at higher risk of committing errors leading to data breaches, such as mishandling sensitive information or falling for phishing scams. Such lapses in security protocols could expose the Force’s data to unauthorised access or disclosure. **(Medium, MA4)**

We noted the following controls to be adequately designed and operating effectively:

Software Asset Management

The Force utilises Microsoft System Center Configuration Manager (SCCM), Flexera, and Microsoft Sentinel. Although none of these are dedicated software and application inventories, they offer a comprehensive view of all software within the network. Furthermore, the Force is currently in the process of implementing a software asset management system, with plans to pilot BellArc next month. Additionally, Flexera is employed to detect any unused or unauthorised software, platforms, and applications. Indicating a proactive approach towards software asset management practices within the Force.

Network Architecture

Network architecture has been thoroughly documented and takes into account the flow of information and the criticality of assets during the design phase. Additionally, segregation and segmentation within the environment have been achieved using VLANs, strategically placed according to geographic location and access requirements. The Force prioritises network integrity, security, and efficiency, aligning its infrastructure design with best practices to safeguard against potential threats and ensure smooth operation of its network environment.

Backups

A backup policy has been established and backups are stored in two separate data centres to provide redundancy. Tapes are duplicated and replicated across both sites. Monthly testing of backups is conducted, and comprehensive records of these tests are meticulously maintained. Furthermore, these backup procedures have been synchronized with tested Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). The Force have implemented comprehensive backup measures to mitigate risks and ensure the continuity of its operations.

✓

Event Data

The National Monitoring Centre (NMC) conducts thorough reviews of all event logs collected and correlated by Microsoft Sentinel. Microsoft Sentinel employs various sources such as servers, external firewalls, and Microsoft 365 to aggregate threat data. Providing benefits from comprehensive monitoring and analysis capabilities provided by Microsoft Sentinel, allowing for a proactive approach to threat detection and response across diverse sources of data.

✓

Anti-Virus

Microsoft Defender serves as the primary antivirus tool deployed on every endpoint. Upon reviewing a Power BI compliance dashboard, it was observed that antivirus is enabled on 100% of devices. Defender is configured to conduct real-time scanning for malicious code. The comprehensive endpoint protection provided by Microsoft Defender, ensures a high level of security against potential malware threats across all devices.

✓

Incident Management

A thorough incident management plan is established, with clearly defined roles and responsibilities for the incident response team. The team has undergone training, and a process for learning from past incidents is implemented. The Force are well-prepared to effectively respond to and manage incidents, with a trained team and a structured approach for continual improvement based on lessons learned from previous incidents.

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.

Area: ID.RA-1: Asset vulnerabilities are identified and documented				
Control	The Force conduct a formal penetration test annually and bi-annual vulnerability tests, however, tracking of vulnerabilities is not being adequately performed.		**Assessment:** **Design** **Compliance**	 x N/A
Findings / Implications	The Force conduct a formal penetration test annually in November, known as an IT Health Check (ITHC). We reviewed a tracker with all findings listed from the ITHC, we noted 39 high findings, 34 medium findings, and the rest either low or informational. Whilst management informed us that work has been conducted to remediate these issues, we noted that the status column of the action tracker has not been adequately completed. Without proper tracking, identified vulnerabilities may remain unaddressed, leading to an incomplete remediation process. This increases the likelihood of known vulnerabilities being exploited by malicious actors, resulting in security breaches, data leaks, or service disruptions. Moreover, we noted that a ticketing system was previously used for tracking vulnerabilities, but now only significant threats go through the ticketing tool and are sent to relevant teams to remediate (e.g., information security or ICT teams). Lower-level vulnerabilities are not being tracked as effectively since the Force transitioned from a ticketing system to using Microsoft Teams lists and spreadsheets for tracking lower-level vulnerabilities, with plans to trial Redmine (project management and issue tracking tool) in a virtual machine. Without a centralised tracking mechanism, there is a risk of losing accountability for addressing lower-rated vulnerabilities. These vulnerabilities may fall through the cracks, with no clear ownership or accountability for remediation actions, leading to delays or oversights in the mitigation process.			
Management Action 1	Management will adequately track the status of findings from the penetration tests and vulnerability scans findings to ensure timely remediation of vulnerabilities and ensure that adequate tooling is utilised to track all vulnerabilities to remediation.	**Responsible Owner:** Information Security Manager	**Date:** 30 September 2024	**Priority:** **Medium**

Area: PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorised devices, users and processes.				
Control	The Force have a standardised process for joiners, movers, and leavers. This utilises a standard Active Director (AD) group control system rather than role based access control. Processes for third party or contractor access have not been documented.		**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	For new personnel and those leaving, the Force follows a standardised process. A joiner's form is submitted, initiating a workflow within Oracle HR. Automated processes at 1 am cross-reference HR data, including exit dates for former employees. Joiners are automatically granted domain logon access with standard information, providing entry to the intranet and basic access to the Y drive. All other systems, require approval from the designated asset owner for access. We note that user access control has been documented within the ICT Infrastructure Information Security Expectations. Access is determined through AD groups, defining specific access levels for individuals based on their HR profiles. The Force utilises a standard AD group control rather than usual role-based access control (RBAC), and we note there is a National IT Project driven by the Home Office to move to a more formal RBAC system with an aim to complete implementation by the end of FY 25/26. Third parties or contractors require access via a request form submitted to the service desk. Access is granted upon the approval of a sponsoring person, typically from the IT department. Access is limited to specific areas, both in terms of where they can access and the designated timeframes for their access. However, the processes for controlling third party access have not been documented within the ICT Infrastructure Information Security Expectations document. Moreover, management did not provide evidence to support compliance with the informal process. Without documented processes for managing third-party access, there is a higher risk of security vulnerabilities. Third parties may gain unauthorised access to sensitive systems, data, or resources, leading to data breaches, unauthorised disclosures, or other security incidents.			
Management Action 2	Management will ensure that processes for third-party access control have been documented.	**Responsible Owner:** Information Security Manager	**Date:** 30 June 2024	**Priority:** Medium

Area: DE.CM-8: Vulnerability scans are performed				
Control	Vulnerability scans are performed on a bi-annual basis via Nessus. Processes for vulnerability scans have not been documented.		**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	We found that Nessus is being utilised as the tooling for vulnerability scanning and these scans are being performed twice a year. However, we note that information pertaining to vulnerability scanning has not been included within the ICT Infrastructure Information Security Expectations document. Without documented processes, vulnerability scanning activities may be inconsistent or inefficiently executed. This can result in missed vulnerabilities, incomplete scans, or inaccuracies in the assessment of the Force's security posture, leaving critical systems and data exposed to potential exploitation.			
Management Action 3	Management will include vulnerability scanning processes within the ICT Infrastructure Information Security Expectations document.	**Responsible Owner:** Information Security Manager	**Date:** 30 June 2024	**Priority:** **Medium**

Area: PR.AT-1: All users are informed and trained

Control

A security awareness training program is in place, utilising web modules, assessments, and awareness newsletters.

Compliance rates with passing modules are lower than expected.

Assessment:

Design	✓
Compliance	N/A

Findings / Implications

The Force have a comprehensive training program, including Force-wide masterclasses, mandatory training courses, periodic reminders of policy broadcasted through the Force broadcast system, and monthly awareness newsletters sent out by the information security team. Moreover, staff in specialised security roles undergo additional training, including two modules on protecting information and the Data Protection Foundation for Information Assurance Officers (IAOs).

The mandatory training courses, include:

- Managing information: both non-operational and operational aspects, depending on job role.
- Introduction to Government Security Classifications.

Participants must answer a set of questions with a pass mark of 80%. The content includes information on data protection and incident management.

An e-learning Power BI system is in place to track training progress. The numbers are reported to the Executive Board, and any non-completion leads to a supervisor response. We reviewed the Power BI dashboard and note that there is a 77% completion rate, for the Managing Information: Operational course, and 54.6% completion rate for Managing Information: Non-Operational for users who have completed the training within the past two years (on a rolling basis). Management highlighted to us that there have been difficulties with achieving relevant buy-in from key stakeholders (e.g., heads of departments, line management). Employees who fail to grasp data protection concepts are more likely to make mistakes that could lead to data breaches. This could include mishandling sensitive information, falling for phishing scams, or failing to follow security protocols, leaving the Force's data vulnerable to unauthorised access or disclosure.

The effectiveness of the security awareness training program is tested through various methods, principally,

- Phishing exercises conducted by the cybercrime team. These exercises involve notifying only a few key IT staff members to simulate real-world scenarios. We reviewed results of the previous phishing exercise and note that 0.18% of users were compromised out of 7,657 users tested, with 0.17% of users reporting. Users are directed to Microsoft Phishing training when they fail a phishing test.
- Management highlighted that there are challenges in incident trend tracking due to incident statistic data being hard to analyse. Therefore, a wider understanding on whether training has affected incident reporting is not achievable. Incident trend tracking is essential for refining incident response procedures and improving the Force's ability to mitigate and contain incidents effectively. Without a clear understanding of past incidents and their underlying causes, the Force may struggle to develop appropriate response strategies or allocate resources efficiently during future incidents.

Area: PR.AT-1: All users are informed and trained				
Management Action 4	Management will implement processes to ensure relevant buy-in from management responsible for ensuring staff completion of information security training.	**Responsible Owner:** Information Security Manager via DDAC	**Date:** 31 October 2024	**Priority:** Medium
Management Action 5	Management will ensure that that incident trend tracking processes are implemented to allow for process improvements, this should include the collation, tracking, and analysis of incident data.	**Responsible Owner:** Information Security Manager	**Date:** 30 September 2024	**Priority:** Low

Area: ID.AM-1: Physical devices and systems within the organisation are inventoried				
Control	The Force utilise VivaTrak for asset management, this is supported by an Excel dashboard which is fed into by Microsoft System Center Configuration Manager (SCCM) and Microsoft Entra. The tooling does not include non-network connected assets.		**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	Asset data is tracked via VivaTrak, an asset management tool. Moreover, the asset management team utilises an Excel dashboard for tracking various assets, including laptops and desktops. This dashboard receives feeds from System Centre Configuration Manager (SCCM), VivaTrak and Microsoft Entra. The team employs triggers via macros for change detection, sourced from SCCM, Flexera, InTune, and reports from Microsoft Entra. The Force maintains a comprehensive inventory of all network-connected assets, encompassing laptops, desktops, and other devices. We reviewed an asset report from VivaTrak, and note that the report includes the asset type, model, condition, location, serial, asset reference, and asset loanee. However, non-network connected assets, such as monitors, are not actively monitored. If non-network connected assets are not being actively monitored or tracked, this could lead to a lack of visibility and control over these physical devices resulting in difficulties in managing the overall asset inventory.			
Management Action 6	Management will actively track and monitor non-network connected assets as part of the asset management programme. Management will determine which assets to formally track (e.g. monitors) and which are to be classed as consumables (e.g. keyboards and mice).	**Responsible Owner:** Head of ICT Services and Operations	**Date:** 31 October 2024	**Priority:** Low

Area: ID.RA-6: Risk responses are identified and prioritised				
Control	The Force's IT department hold an Information Security risk register, however, mitigating actions within the Information Security risk register have not been allocated target due dates.		**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	We reviewed the Force's IT department's Information Security risk register. This register includes major IT risks, encompassing six force-level risks and five major security risks. The team conducts an annual process involving meetings with information asset owners. Following these meetings, areas compliant with the security environment are identified, and any issues are escalated to Head of IT and added to the Information Security risk register. We found that all risks are allocated priorities, risk owners, and mitigating actions. However, we note that risk management mitigating actions are not allocated target due dates. Without clear deadlines, there may be a loss of focus on risk mitigation efforts. Team members may lack a sense of urgency or direction, resulting in inefficient use of resources and missed opportunities for proactive risk management.			
Management Action 7	Management will include target due dates for mitigation actions within the Information Security risk register.	**Responsible Owner:** Information Security Manager	**Date:** 28 February 2025	**Priority:** **Low**

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	5 (16)	1 ** (16)	3	4	0
Total			**3**	**4**	**0**

* 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.

** More than one management action has been raised against a control.

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 objective:

Objective of the risk under review	Risk relevant to the scope of the review	Risk source
To provide assurance that the processes in place to manage cyber security risk are effective.	Risk Reference: 1685	Risk Register

When planning the audit, the following areas for consideration and limitations were agreed:

The objective of this audit is to evaluate the design of key cyber security controls in place and test the operating effectiveness of selected controls within the following domains as defined in the NIST (US National Institute of Standards and Technology) cyber security framework:

IDENTIFY
What processes and assets need protection?

PROTECT
What safeguards are available?

DETECT
What techniques can identify incidents?

RESPOND
What techniques can contain impacts of incidents?

RECOVER
What techniques can restore capabilities?

The audit will consider the following;

Identify (ID):

Governance (ID.GV)

- ID.GV-1: Organisational cybersecurity policy is established and communicated.

Asset Management (ID.AM)

- ID.AM-1: Physical devices and systems within the organisation are inventoried.
- ID.AM-2: Software platforms and applications within the organisation are inventoried.

Risk Assessment (ID.RA)

- ID.RA-1: Asset vulnerabilities are identified and documented.
- ID.RA-6: Risk responses are identified and prioritised.

Protect (PR):

Identity Management, Authentication and Access Control (PR.AC)

- PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorised devices, users and processes.
- PR.AC-4: Access permissions and authorisations are managed, incorporating the principles of least privilege and separation of duties.
- PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)

Awareness and Training (PR.AT)

- PR.AT-1: All users are informed and trained.

Information Protection Processes and Procedures (PR.IP)

- PR.IP-4: Backups of information are conducted, maintained, and tested.

Detect (DE):

Anomalies and Events (DE.AE)

- DE.AE-3: Event data are collected and correlated from multiple sources and sensors.

Security Continuous Monitoring (DE.CM)

- DE.CM-4: Malicious code is detected.
- DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.
- DE.CM-8: Vulnerability scans are performed.

Respond (RS):

Communications (RS.CO)

- RS.CO-1: Personnel know their roles and order of operations when a response is needed.

Mitigation (RS.MI)

- RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.

Limitations to the scope of the audit assignment:

- The approach taken for this review will be to validate the design of key controls within the scope and will not include all monitoring controls.
- We will be testing only selected key controls and on a sample basis only.
- We will not perform penetration tests and vulnerability assessments however we will review the results of tests undertaken by independent service providers and their reporting to the Force.
- Our work in relation to recovery aspects will only be specific to cyber incidents and not Force wide operational resilience.
- 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 cyber security environment, and it will be necessary for management to consider the results and make their own judgement on the risks affecting the Force and the level of specialist computer audit coverage they require in order to provide assurance that these risks are minimised.
- The results of our work are reliant on the quality and completeness of the information provided to us.
- Our work does not provide an absolute assurance that material error; loss or fraud does not exist.

Debrief held	4 April 2024
Draft report issued	22 April 2024
Revised draft report issued	30 May 2024
Responses received	21 June 2024
Final report issued	21 June 2024

Internal audit contacts	Dan Harris, Head of Internal Audit (IA) Philip Church, Associate Director IA Hollie Adams, Assistant Manager IA Steven Snaith, Technology Risk Assurance (TRA) Lead Wil Milligan, Manager TRA Kiran Solanki, Manager TRA
Client sponsor	Director of Finance and Assets Head of ICT Head of ICT Service and Operations
Distribution	Director of Finance and Assets Head of ICT Head of ICT Service and Operations Information Security Manager

We are committed to delivering an excellent client experience every time we work with you. If you have any comments or suggestions on the quality of our service and would be happy to complete a short feedback questionnaire, please contact your RSM client manager or email admin.south.rm@rsmuk.com

rsmuk.com

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of **The Chief Constable of Cleveland**, and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM UK Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM UK Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM UK Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.