THE POLICE AND CRIME COMMISSIONER FOR CLEVELAND AND THE CHIEF CONSTABLE OF CLEVELAND

Follow Up of Previous Internal Audit Management Actions: Visit 2

Final Internal audit report 11.22/23
7 March 2023

1. EXECUTIVE SUMMARY

Background

The focus of this review is to provide assurance that agreed management actions have been fully implemented. These are in respect of the following internal audit reports that have been completed by RSM:

- Automatic Number Plate Recognition (ANPR) (10.20/21);
- Positive Action (Workforce Representation, Attraction, Recruitment, Progression and Retention) (15.20/21);
- IT Asset Management (18.20/21);
- Data Quality Process (Crime Recording) – Force Audit and Monitoring Mechanisms (3.21/22);
- Follow up of Previous Internal Audit Management Actions: Visit 1 (6.21/22);
- Sickness Absence (Including Medical Retirement) (7.21/22);
- Equality, Diversity and Inclusion (8.21/22);
- Victims' Code (9.21/22);
- Follow Up of Previous Internal Audit Management Actions: Visit 2 (13.21/22);
- Force Control Room (15.21/22);
- Vetting (1.22/23);
- Firearms Licensing (2.22/23);
- Cyber Security Review (3.22/23);
- Key Financial Controls (5.22/23);
- Health and Safety (6.22/23); and
- General Data Protection Regulation (GDPR) (7.22/23).

The Force has reported a total of 38 management actions as complete from the above reports, comprising of three high, 21 medium and 14 low priority management actions.

Conclusion

We were provided with satisfactory evidence in respect of two high, 19 medium and 13 low priority management actions declared as complete by the respective action owners, and we therefore agreed that these actions had been fully implemented.

We have categorised two of the four management actions as ongoing and have categorised the final two management action as superseded. Details of the ongoing management actions can be found under section two of this report, and details of the superseded management action can be found under Appendix B. We have partially reiterated the two ongoing management actions and categorised these actions as medium priority (noting one was originally a high priority action – which has allowed us to provide the overall progress assurance below).

Taking account of these findings and in line with our definitions set out in Appendix A, in our opinion the organisation has demonstrated **good progress** in implementing agreed management actions.

Progress on actions

The following table includes details of the status of each management action:

Implementation status by category of action	Number of actions agreed	Status of management actions			
		Implemented	Implementation ongoing	Not implemented	Superseded
Low	14	13	0	0	1
Medium	21	19	1	0	1
High	3	2	1	0	0
Total:	**38 (100%)**	**34 (90%)**	**2 (5%)**	**0 (0%)**	**2 (5%)**

2. FINDINGS AND MANAGEMENT ACTIONS

Status	Detail
1	The entire action has been fully implemented.
2	The action has been partly though not yet fully implemented.
3	The action has not been implemented.
4	The action has been superseded and is no longer applicable.
5	The action is not yet due.

Assignment: Cyber Security Review (3.22/23)				
Original management action / priority	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 - National Cyber Security Centre) is used as a baseline for this. In addition, management will logically enforce stronger password requirements for privileged accounts. Priority: **High**			
Audit finding / status	We were provided with a print screen of the password policy configuration which has been enforced on all policing equipment to ensure passwords are updated every 90 days, and must include at least 10 characters, two special characters (such as : ?,!) and numbers. As an additional layer of security, the Force has implemented a password generator which all staff can use to ensure their passwords meet the complexity requirements. We were also provided with the password configuration rationale from the Information Security Manager, which outlines the requirements for password security in line with the best practice guidance from the NCSC. However, we made attempts to discuss how management has enforced the stronger password requirements for privileged accounts, but the Information Security Manager was unavailable during the audit, therefore we cannot confirm whether this action is fully complete. 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. As the Force has taken steps to address the original management action, we have re-categorised the partially reiterated management action as medium priority. **2. The action has been partly though not yet fully implemented.**			
Management Action 1	**Partial reiteration of original management action:** Management will logically enforce stronger password requirements for privilege accounts.	**Responsible Owner:** Information Security Manager	**Date:** 31 August 2023	**Priority:** **Medium**

Assignment: Cyber Security Review (3.22/23)				
Original management action / priority	Management will continue the exercise of allocating DPIAs (data protection impact assessments) and filling gaps and missing fields within the IAR (information asset register). 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). Priority: **Medium**			
Audit finding / status	We obtained a copy of the IAR within the SharePoint system, we noted from reviewing the register 88 assets were still without a DPIA and only 39 had a completed DPIA. From the review of the original report, no further DPIAs have been completed since the previous audit and the latest version would suggest this part of the action has not been implemented. However, we noted through discussions with the Data Protection Officer that they had only recently been appointed to the role in December 2022 and this would be picked up as part of their role going forward. From our review of the IAR, we identified within column M 'classification category' outlines the associated risk to each asset and considers whether the risk associated with each asset falls within the following categories: 1. Failover technology to resume service within six hours; 2. Ability to re-create services from backup within 24 hours; and 3. Remaining applications with business continuity plans in place for up to five days. Each asset is categorised to highlight the critical factor, risk, and impact of disruption. From the original action, we were able to confirm the critical classification codes has been implemented within the IAR and clearly identifies the business risk rating area; however, as the DPIA process is yet to be completed, we have therefore categorised this management action as ongoing. **2. The action has been partly though not yet fully implemented.**			
Management Action 2	**Partial reiteration of original management action:** Management will continue the exercise of allocating DPIAs and filling gaps and missing fields within the IAR.	**Responsible Owner:** Information Governance Manager	**Date:** 31 August 2023	**Priority:** **Medium**

APPENDIX A: DEFINITIONS FOR PROGRESS MADE

The following opinions are given on the progress made in implementing actions. This opinion relates solely to the implementation of those actions followed up and does not reflect an opinion on the entire control environment.

Progress in implementing actions	Overall number of actions fully implemented	Consideration of high priority actions	Consideration of medium priority actions	Consideration of low priority actions
Good	75% +	None outstanding.	None outstanding.	All low actions outstanding are in the process of being implemented.
Reasonable	51 – 75%	None outstanding.	75% of medium actions made are in the process of being implemented.	75% of low actions made are in the process of being implemented.
Little	30 – 50%	All high actions outstanding are in the process of being implemented.	50% of medium actions made are in the process of being implemented.	50% of low actions made are in the process of being implemented.
Poor	< 30%	Unsatisfactory progress has been made to implement high priority actions.	Unsatisfactory progress has been made to implement medium actions.	Unsatisfactory progress has been made to implement low actions.

APPENDIX B: ACTIONS COMPLETED OR SUPERSEDED

From the testing conducted during this review we have found the following actions to have been fully implemented or superseded.

Assignment title	Management actions
Automatic Number Plate Recognition (ANPR) (10.20/21)	Status: **Implemented** A policy will be written and implemented to ensure that the requirements of NASPLE are addressed and this will be communicated to all relevant staff. Priority: **Medium**
Automatic Number Plate Recognition (ANPR) (10.20/21)	Status: **Implemented** A process will be introduced to ensure that when a camera has been in place for 12 months, a DPIA will be completed on the anniversary date (12 months) of its deployment. Priority: **Low**
Automatic Number Plate Recognition (ANPR) (10.20/21)	Status: **Superseded** The Information Management Policy and the Information Security Policy will be revised to ensure that Cleveland Police are complying with the National Standards and then reissued. In the event a separate ANPR Policy is implemented these two policies will still need to reflect the ANPR requirements of NASPLE. Priority: **Low** *The Force have not updated the Information Management Policy as it would incur mass amounts of additional work internally and would result in a policy which would consist of multiple scenarios to understand the NASPLE requirements, but it would be of no relevance to internal staff. We have therefore agreed to supersede the management action.*
Automatic Number Plate Recognition (ANPR) (10.20/21)	Status: **Implemented** An audit plan will be developed alongside the introduction of the Auditor to ensure that all auditable areas are addressed and the procedure for auditing is documented. The audit plan will be implemented, and an audit conducted, every six months to ensure that Cleveland Police are compliant with all areas of the standards. Priority: **Low**

Assignment title	Management actions
Positive Action (Workforce Representation, Attraction, Recruitment, Progression and Retention) (15.20/21)	Status: **Implemented** The Force will develop an action and delivery plan for positive action to outline actions in respect of the NPCC toolkit. Actions will be assigned appropriate responsible owners in line with the three strategic workstreams: • Organisation and People; • Communities; and • Partnerships. Progress against the actions will be regularly reported to EDI Board. Priority: **Medium**
Positive Action (Workforce Representation, Attraction, Recruitment, Progression and Retention) (15.20/21)	Status: **Implemented** The Recruitment Manager will ensure that members of selection panels are documented. Priority: **Medium**
Positive Action (Workforce Representation, Attraction, Recruitment, Progression and Retention) (15.20/21)	Status: **Implemented** The promotion and utilisation of cultural exchange programs within law enforcement will be considered as part of the Force's leadership training needs analysis review. Priority: **Low**
Positive Action (Workforce Representation, Attraction, Recruitment, Progression and Retention) (15.20/21)	Status: **Implemented** The Head of HR will develop a confidential review process for selection, grievances, and misconduct-related processes in respect of protected characteristics to ensure a lessons learnt approach is adopted and documented. Additional advice will be provided from the EDI Team. Priority: **Low**
IT Asset Management (18.20/21)	Status: **Implemented**

Assignment title	Management actions
	Management will ensure that all assets are returned when staff move or leave the Force. Regular spot checks should be performed to ensure that this happens. Priority: **Medium**
IT Asset Management (18.20/21)	Status: **Implemented** Management will ensure that a formal capacity management and IT asset replacement strategy covering all IT assets is defined, approved, and implemented. Priority: **Medium**
IT Asset Management (18.20/21)	Status: **Implemented** Management will ensure that they conduct regular audits/stock checks of the IT hardware assets. Priority: **Medium**
IT Asset Management (18.20/21)	Status: **Implemented** Management will ensure that the IT asset management process is updated to include as a minimum: 1. Roles and responsibilities; 2. Mechanisms for recording and tracking IT assets; 3. IT asset audits and their frequency; and 4. IT asset lifecycle process. Priority: **Medium**
Data Quality Process (Crime Recording) – Force Audit and Monitoring Mechanisms (3.21/22);	Status: **Implemented** Once the Force Crime Management Unit is developed, the Force will implement standard operating procedures for crime recording to ensure that officers are informed of processes and expectations specific to Cleveland Police. Priority: **Low**
Follow up of Previous Internal Audit Management Actions (6.21/22)	Status: **Implemented**

Assignment title	Management actions
	ICT will ensure that the ICT testing plan is documented, future testing is recorded, and documentation is available to support the results of the regular testing. Test results will be documented as part of a formal test report which details test objectives, outcomes, and lessons learned and be used in updating the associated ICT DR plans and supporting documents. Priority: **Medium**
Follow up of Previous Internal Audit Management Actions (6.21/22)	Status: **Implemented** The Head of ICT will complete a review of existing system recovery procedures to determine whether they have been reviewed recently and the review process can be incorporated into business as usual activity. Priority: **Medium**
Follow up of Previous Internal Audit Management Actions (6.21/22)	Status: **Implemented** Results of the self-assessment will be reported to the People and Wellbeing Board to ensure appropriate monitoring of actions. Priority: **Low**
Follow up of Previous Internal Audit Management Actions (6.21/22)	Status: **Implemented** The updated People and Wellbeing Board reports will be produced in which key statistics will be outlined and included in monthly reports to provide up to date information. Priority: **Low**
Sickness Absence (Including Medical Retirement) (7.21/22)	Status: **Implemented** The Force will undertake an exercise to assess the impact and cost of sickness absence over the financial year 2021/22. Priority: **Medium**
Sickness Absence (Including Medical Retirement) (7.21/22)	Status: **Implemented** We will ensure that specific training in attendance management is rolled out as part of the leadership training for newly appointed line managers.

Assignment title	Management actions
	Priority: **Low**
Equality, Diversity and Inclusion (8.21/22);	Status: **Implemented** The Force should develop a policy that uses the Force's strategic objectives to set out the requirements of the PSED. Priority: **Low**
Equality, Diversity and Inclusion (8.21/22);	Status: **Implemented** The EDI Board will ensure the action log is fully updated and contains an estimated completion date for all actions. Priority: **Medium**
Victims' Code (9.21/22)	Status: **Implemented** The Crime Data Integrity Victims and Witness Strategic Governance Group will ensure recommendations within reports submitted to them are recorded and followed up. This will be undertaken by the Chair of the Group. In addition, the results of the internal audit report will be feed into the Inspection and Audit Monitoring Board. Consideration will also be given to the introduction of a Risk, Action, Issues and Decision log to reflect the activity more accurately within each meeting. Priority: **Medium**
Victims' Code (9.21/22)	Status: **Implemented** An action plan and timetable will be set out to increase training compliance to an agreed level closer to the overall 100% target, with due allowance for staff absence and other unavailability. Priority: **Medium**
Follow Up of Previous Internal Audit Management Actions: Visit 2 (13.21/22)	Status: **Superseded** Upon the implementation of online IT asset disposal forms, the Force will ensure that confirmation checks regarding an asset's preparation and relocation to a designated disposal area are complete within a timely basis

Assignment title	Management actions
	Priority: **Medium** *The Force has considered the original action as implemented; however, they have developed an alternative approach where the original action is no longer deemed relevant. The Force has instead implemented a live IT asset disposal register within SharePoint, which records and monitors all disposals of assets across the Force and allows for a centralised recorded to be held for reporting purposes.*
Force Control Room (15.21/22);	Status: **Implemented** All individuals on the training needs analysis document will have all their applicable training populated. Priority: **Low**
Vetting (1.22/23)	Status: **Implemented** The Vetting Team will ensure all individuals with MV and NPPV-3 clearance have a 28 and 56 month review scheduled on the Corevet system and these are completed in a timely manner. Priority: **Medium**
Vetting (1.22/23)	Status: **Implemented** The Force will ensure that the resources approved as part of the resource paper are recruited to address the backlog of expired vetting and upcoming expiring vetting. The Force will: • Undertake a reconciliation exercise of the vetting backlog to determine whether vetting requests are still required; • develop an action plan to address the vetting backlog, including prioritisation of vetting requests using a risk-based approach to ensure the backlog is methodically approached; and • provide regular reporting to SMT on the progress in addressing the backlog of vetting requests. Priority: **High**
Vetting (1.22/23)	Status: **Implemented** Discussions will be undertaken to determine whether the data retention function on Core-vet can be implemented. If it can, then a plan will be created outlining how this will be implemented. Priority: **Medium**

Assignment title	Management actions
Firearms Licensing (2.22/23);	Status: **Implemented** The Force will update and circulate the summary operational procedure document to relevant staff within the Force. Priority: **Low**
Firearms Licensing (2.22/23);	Status: **Implemented** The Force will ensure evidence of training undertaken by the Firearms Licensing Unit is retained to support the role of the Unit. Priority: **Low**
Firearms Licensing (2.22/23);	Status: **Implemented** The Force will provide additional training to the Firearms Licensing Unit on the process to ensure compliance with the Home Office statutory guidance. Priority: **Medium**
Firearms Licensing (2.22/23);	Status: **Implemented** The Force will update the Firearms Licensing Policy to outline its responsibilities with regard to compliance with data protection legislation as required by the Home Office statutory guidance. Priority: **Medium**
Key Financial Controls (5.22/23);	Status: **Implemented** The Force will ensure all staff are made aware of the purchase order authorisation process for any goods or services. Priority: **Low**
Health and Safety (6.22/23)	Status: **Implemented** The Health and Safety Manager will raise the issue of health and safety reporting and governance arrangements within the Force with the intention of implementing regular Force reporting on health and safety matters to an appropriate committee or Group.

Assignment title	Management actions
	Priority: **High**
General Data Protection Regulation (GDPR) (7.22/23)	Status: **Implemented** a) Earlier intervention will take place to identify asset owners to ensure they understand their responsibilities. b) Email prompts will be issued to all asset owners on a quarterly basis to identify if owners or guardians have changed. Priority: **Medium**
General Data Protection Regulation (GDPR) (7.22/23)	Status: **Implemented** A formal internal procedure will be produced in relation to SARs and the deletion of data to ensure that individuals' expectations are met, and all members of the team are aware of their responsibilities in relation to GDPR. Priority: **Medium**

APPENDIX C: SCOPE

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

Objective relevant to the scope of the review

Objective of the area under review
To ensure that agreed recommendations / management actions raised by internal audit have been actioned by management in a timely manner.

Scope of the review

The focus of this review is to provide assurance that recommendations / management actions previously reported have been fully implemented. We will consider actions that have been closed since the previous internal audit follow up review which was undertaken in August 2022.

The following limitations apply to the scope of our work:

- The review will only cover audit recommendations / management actions previously made, and we will not review the whole control framework. Therefore, we will not provide assurance on the entire risk and control framework.
- We will ascertain the status of recommendations / management actions through discussion with management and review of the recommendation tracking.
- Where the indication is that recommendations / management actions have been implemented, we will undertake limited testing to confirm this.
- Where testing has been undertaken, our samples will be selected over the period since actions were implemented or controls enhanced.
- Our work does not provide any guarantee or absolute assurance against material and/or other errors, loss or fraud.

Debrief held	20 January 2023	**Internal audit Contacts**	Dan Harris, Head of Internal Audit
Secondary Debrief held	1 March 2023		Philip Church, Senior Manager
Draft report issued	6 March 2023		Hollie Adams, Assistant Manager
Responses received	7 March 2023		Naomi Longstaff, Internal Auditor
Final report issued	7 March 2023	**Client sponsor**	HMIC Liaison Officer
		Distribution	HMIC Liaison Officer

rsmuk.com