Agenda Item 06

west midlands
police and crime
commissioner

INTERNAL AUDIT ACTIVITY REPORT

Joint Audit Committee
26 March 2026

LYNN JOYCE
HEAD OF INTERNAL AUDIT

PURPOSE OF REPORT

The purpose of this report is to update the Committee of the progress of internal audit activity and summarise the key control issues arising for those audits undertaken for the period December 2025 to date.

The Joint Audit Committee's Terms of Reference includes a requirement to receive progress reports on the activity of Internal Audit. This activity report provides the following:

- Plan progress summary;
- Summary of audits receiving Limited or Minimal assurance opinion;
- Summary of other assurance activity completed;
- Proposed changes to the audit plan;
- Recommendations analysis; and
- Performance update.

The role of Internal Audit is to provide members and managers with independent assurance on the effectiveness of controls that are in place to ensure that the Police and Crime Commissioner and Chief Constable's objectives are achieved. The work of the Team should be directed to those areas and risk which will most impact upon the Police and Crime Commissioner and Chief Constable's ability to achieve these objectives.

Upon completion of an audit an assurance opinion is given on the soundness of the controls in place. The results of the entire audit programme of work culminate in an annual audit conclusion given by the Head of Internal Audit based on the effectiveness of the framework of risk management, control and governance designed to support the achievement of the organisations objectives.

RECOMMENDATIONS

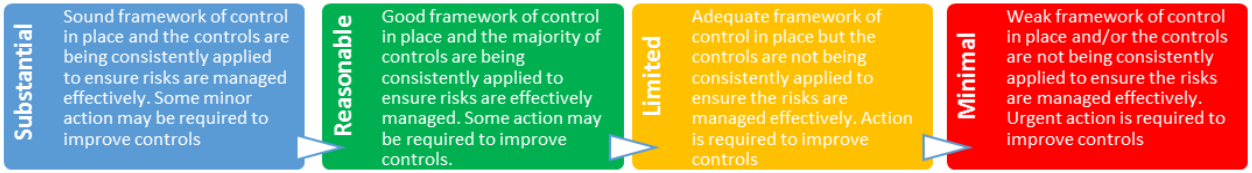
The Committee note the material findings in the attached Internal Audit Activity Report and the performance of the Internal Audit Service and support the proposed changes to the Internal Audit Plan.

CONTACT OFFICER
Name: Lynn Joyce
Title: Head of Internal Audit

BACKGROUND DOCUMENTS
None

PLAN PROGRESS SUMMARY

Our aim is to provide independent assurance that the organisation's risk management, governance and internal control processes are operating effectively. We provide an assurance opinion at the conclusion of each internal audit which is derived from the work undertaken and is intended to provide senior management with a level of assurance about the internal controls in place in that particular system or activity. The audit opinions currently used are:



The table below captures the planned audits for 2025/26, along with their current status and opinions. Seven audit reports were finalised during the reporting period, one of which received a Minimal opinion. Four audit reports are currently in draft awaiting management comments.

The pages that follow summarise those audits that received minimal or limited assurance, including Information Governance and Civil Litigation Claims and Insurance which were reported in the previous quarter, which the JAC requested to revisit this quarter.

Audit	Status	Opinion
Insurance	Final	Limited
IT Application Management	Final	Reasonable
Financial Savings Governance	Final	Limited
Neighbourhood Policing Engagement	Final	Limited
VAWG Delivery Planning	Final	Limited
IT&D Database Access and Administration	Final	Reasonable
Information Governance and Decision Making	Final	Minimal
Dog Unit	Final	Limited
Civil Contingencies	Draft	
Central Ticketing Office	Final*	Minimal
Force Contact Resourcing	In progress	
Benefits Realisation	Draft	
Social Media Strategy	Final	Reasonable
Grievance Process	Final	Reasonable
Contingent Workers	Draft	
Records Management /Compliance with MOPI	Draft	
Robotics Governance	Final*	Reasonable
Cyber Security	In progress	

Audit	Status	Opinion
Income Generation – Driver Improvement Courses	In progress	
Gifts and Hospitality (OPCC)	Final	Reasonable
Gifts and Hospitality (Force)	Final	Reasonable
Fleet Maintenance	Postponed	N/A
Forensic Medical Statements	In progress	
Payroll	In progress	
Cash Office Functions	Final*	Reasonable
Bank Reconciliation	Final	Substantial
VAT	Final	Substantial
Risk Management	Final*	Substantial
ROCU Serious and Organised Crime	Cancelled	N/A
CTU Business Services Team	Final*	Reasonable
LPA Governance, Data and Performance (Dudley)	Final*	Substantial
LPA Governance, Data and Performance (Walsall)	Final*	Substantial
OPCC Casework	Final	Limited
My Community Fund	Final	Reasonable
Regional Economic Crime Unit – Fraud (NEW)	To start	

**Finalised during reporting quarter*

MINIMAL OPINION AUDIT – Central Ticket Office

Objectives and Scope

This review focused on the arrangements in place within the Central Ticket Office for the processing of Notices of Intended Prosecution (NIP) and Section 172 notices to ensure legal compliance. The areas reviewed were:

- Governance and performance monitoring arrangements, including policies and procedures; reporting lines, oversight responsibilities and reporting.
- Compliance, including legal duty requirements, record keeping to demonstrate that appropriate eligibility checks where conducted on drivers, and relevant records updated, e.g. conditional offer letter, etc.
- Training arrangements to ensure those processing NIPs and Section 172 notices have received appropriate training to fulfil their responsibilities.

Overall Opinion

MINIMAL ASSURANCE

(Definitions of ratings are provided at Appendix A)

There is a weak framework of control in place and/or the controls are not being consistently applied to ensure the risks are managed effectively.

Urgent action is required to improve controls.

Number of Actions	
High	2
Medium	4
Low	1
Total	7

Conclusion

The Central Ticket Office (CTO) has recently undergone an annual work uplift of 67% for 2025/26, driven by commitments under the Vision Zero Strategy which focuses on reducing road deaths and serious injuries through stronger enforcement. However, due to a lack of adequate resource and project planning prior to the implementation of enforcement measures, increased pressure has been placed on the existing workforce resulting in backlogs and delays in ticket processing. Consequently, a significant number of tickets are being cancelled as they have become statute barred, following the expiry of the six-month limitation period to initiating legal proceedings.

CTO are currently going through a recruitment exercise to increase staff numbers and are exploring a number of measures to manage resource constraints. However, there are lapses in the governance framework, both in addressing the existing backlog and in overseeing the actions designed to reduce and prevent further backlogs, which is reflected in the minimal opinion.

Good Practice

- CTO perform reconciliations on StarTraq files (video files capturing motoring offences) when they are imported into PentiP (fixed penalty notice system utilised by the Force), ensuring data transfer is whole and complete.
- Accuracy checks are conducted during printing and mail-merge processes of NIPS and Section 172 notices to reports generated from PentiP, to ensure that correct documents are being sent to the intended recipient.
- An up-to-date business continuity plan has been established for CTO, providing a framework for the Force to identify potential disruptions, analyse impact on critical functions and service delivery, and define actions to maintain or restore operations to an acceptable level.

Key Findings Summary

High	A lack of effective resource and project planning, combined with an uplift of annual work for CTO, has created a resource constraint. This has resulted in a backlog of work which has negatively impacted service delivery and significantly increased the number of cancelled tickets.
Medium	No monitoring framework has been established to assess performance of individual staff within CTO. Management are therefore unable to gauge progress made by individuals and/or explore the reasons for performance issues to determine if any improvement actions are required.
Medium	Action plans devised to address Camera Enforcement Unit (CEU)/CTO performance do not capture key information such as revised target dates, completion dates and approvals for closure of actions, negatively impacting management oversight and accountability.
High	Key performance indicators currently being reported for CTO are not appropriate, as they do not adequately reflect current resource constraints and operational bottlenecks within the department. This limits management visibility of total workload and operational efficiency.
Medium	Access to the PentiP system has remained active for staff that have left or transferred from the CTO department, increasing the risk of unauthorised access.
Medium	There is a lack of segregation of duties within the ticket cancellation process. Temporary staff are able to cancel tickets, increasing the risk of incorrect cancellations.
Low	Individual training records are not maintained, and team records only capture internal training sessions delivered without key details such as completion date, which limits evidence of competencies of staff.

LIMITED OPINION AUDIT – Civil Litigation Claims and Insurance *(Originally reported in December 2025)*

Objectives and Scope

The audit aimed to provide assurance that the Insurance function is efficiently and effectively managed, and that there is an appropriate level of rigor and challenge around insurance and civil litigation claims. The areas covered included:

- Policies and procedures to support the efficient and effective operation of the insurance and civil litigation functions.
- A review of the claims handling processes for Employers Liability, Public Liability and Motor claims, including an assessment of the level of rigour and challenge around claims and the level of supporting documentation retained.
- Arrangements in place to allow effective cross-working and sharing of information between the Insurance Team and related functions such as Fleet and the Civil Litigation Team.
- Potential improvements in VFM on insurance/legal claims processes.
- Governance, oversight and reporting mechanisms to ensure senior leadership has a clear line of sight with respect to the management of insurance.

Overall Opinion		Number of Actions	
 LIMITED ASSURANCE	There is an adequate framework of control in place, but the controls are not being consistently applied to ensure the risks are managed effectively Action is required to improve controls	High	0
		Medium	4
		Low	1
		Total	5

Conclusion

Several factors contributed to the Limited opinion. Opportunities were identified to strengthen governance and cross-working arrangements across the various teams involved in handling insurance claims to allow for better sharing of information, improved performance monitoring through wider ranging KPIs, and more accurate forecasting of liability claims.

From discussions during the audit, the Insurance and Civil Litigation Teams were aware of some data accuracy issues on the system for some Public Liability claims. Improving the governance and cross working arrangements could further strengthen the controls in place to avoid further instances.

Good Practice

- Financial Regulations clearly set out the responsibility of the Force Chief Finance Officer (FCFO) for the day-to-day operational control and management of all insurance funds, identifying the level of associated claims, and authorising expenditure from the Fund. The Financial Regulations also include the responsibilities for the settlement of civil claims, and the FCFO's annual review of insurance arrangements.
- Sample testing of motor claims confirmed that in each instance, appropriate supporting documentation, including invoices, estimates for repairs, and the notification document containing details of the incident, were held on SharePoint and accessible by the Insurance Team. The accident report was also held on the portal in each instance, evidencing details of the investigation.
- Evidence of ongoing communications with the insurer, the driver, and Fleet were held on file, as applicable.

Key Findings Summary

	A draft Liability Claims Process Chart is in place within the Insurance Team. At the time of audit this was a proposed process only, covering the key stages involved in claims handling from receipt to investigation. It reflects the processes in place as far as Employer's Liability Claims are concerned but is not currently applicable to Public Liability or Motor Claims.
	Similarly, the Civil Litigation Team hold an Information Guide and a Managers' Guide which outline the processes to be followed internally for the handling of Public Liability Claims. The documents did not include processes for cross-working with the Insurance Team.
	From review of a sample of open and closed Employers' Liability Claims notified in the previous 12 months, one claim had originally been set up incorrectly through the Civil Litigation Team as a Public Liability Claim. Whilst this was just one of a wider sample, such examples could result in mishandling of insurance claims. Strengthening policies, governance and cross working arrangements may help avoid similar occurrences.
	Whilst random sampling of Public Liability claims did not raise any anomalies in case handling, historic examples were discussed during the audit where issues had previously been identified between the Insurance and Civil Litigation Teams which largely relate to inconsistencies in dates, errors in

LIMITED OPINION AUDIT – Civil Litigation Claims and Insurance (Continued)

	names or duplication in information recorded. Strengthening cross working arrangements, including reviewing system access between teams, could further help mitigate such errors or support early identification bringing to bear the different expertise and experience of both teams.
	A quarterly Insurance Fund Forecast is completed by the Head of Insurance, recording outstanding reserves for Employer's Liability, Public Liability and Motor Claims, the average payment per quarter, and any anticipated large payments. Due to the absence of more frequent updates between forecasts, this appeared to be leading to issues with maintaining the accuracy of the forecast.
	Currently, formal oversight arrangements do not sufficiently allow for the coming together of the Insurance and Civil Litigation Teams and the FCFO to discuss large value and high-risk claims with the Director of Legal Services, although this does happen on a more informal basis. Also, the FCFO is not fully sighted on all KPIs across both Civil Litigation and insurance functions. Introducing a suitable governance and performance management regime would mitigate this risk.

MINIMAL OPINION AUDIT – Information Governance *(Originally reported in December 2025)*

Objectives and Scope

The audit aimed to provide assurance that there is an appropriate Information Governance Framework in place within the Force. The areas covered were:

- Policies and procedures regarding Information Governance, taking account of authorised professional practice guidance from the College of Policing.
- Documented roles and responsibilities, including accountability structures and responsibilities of the Senior Information Risk Owner (SIRO.)
- Training provided to all individuals including advanced training for those with specific information governance responsibilities.
- Assessment of compliance against the guidance/frameworks in place.
- Incident management logging, including record keeping of incidents, and those which require reporting to the Information Commissioner's Office (ICO.)
- Mechanisms for lessons learnt resulting from breaches, and the organisation's approach to addressing reprimands, recommendations, or enforcement actions that may have been issued by the ICO.
- Governance and reporting mechanisms, include reporting to the Data Assurance and Analytics Board, and Risk and Organisational Learning Board.

Overall Opinion

MINIMAL ASSURANCE

There is a weak framework of control in place and/or the controls are not being consistently applied to ensure the risks are managed effectively.

Urgent action is required to improve controls

Number of Actions	
High	2
Medium	7
Low	1
Total	**10**

Conclusion

The minimal assurance opinion reflects a lack of clear, relevant, and up to date guidance relating to information governance, as well as a number of exceptions identified in the records maintained which increases the risk of data breaches and mismanagement of information.

Management have started their journey to develop a full suite of policies and a new incident management portal to address some of the gaps identified during this audit.

Good Practice

- The Force has an ICO notification chart which helps inform whether an incident should be reported to the ICO. This includes the assessment of the impact on data subject (actual or likely), sensitivity of data, amount of data subjects affected (volume). Scores are assigned to sensitivity and volume of data which when added provide the result of the assessment.
- The Force has an incident management log in place on SharePoint – interlinked with the incident reporting form. Incidents are automatically added to the log when an incident form is submitted.
- The Data Assurance Analytics Board (DAAB), chaired by the Assistant Chief Constable (Deputy SIRO), has an up-to-date Terms of Reference in place. The DAAB's responsibilities include ensuring any data breaches or other data related critical incidents are responded to effectively and any learning is identified and implemented to minimise future risks.
- Effective from October 2024, the Force established Managing Information training for all staff on e-learning. This is scheduled to be annual training, with compliance monitored and reported to the DAAB.
- The Data Protection Officer (DPO) maintains a tracker for monitoring open and closed ICO recommendations, including those from reprimands. Data captured includes ICO reference, recommendation details, current position, outstanding action, status as open or closed, date of closure where relevant.

Key Findings Summary

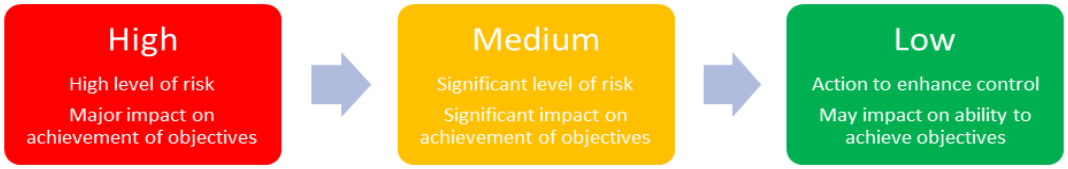
	Whilst we confirmed that the Force has a number of information governance policies in place, they were not up to date and were not being reviewed regularly. Also, in line with the Authorised Professional Practice (APP) for policing, we found a number of gaps within the current guidance, including a lack of an Information Management Strategy.
	Roles and responsibilities were not clearly defined for all staff levels within the Information Security Policy, Freedom of Information Policy and Records Management Policy. Staff may therefore be unaware of their responsibilities.
	Prior to October 2024, there was no periodic training provided to staff on information governance. As of 25 March 2025, compliance was 76.9% against target of 97%, and we confirmed that DAAB had noted concern around this.

MINIMAL OPINION AUDIT – Information Governance (continued)

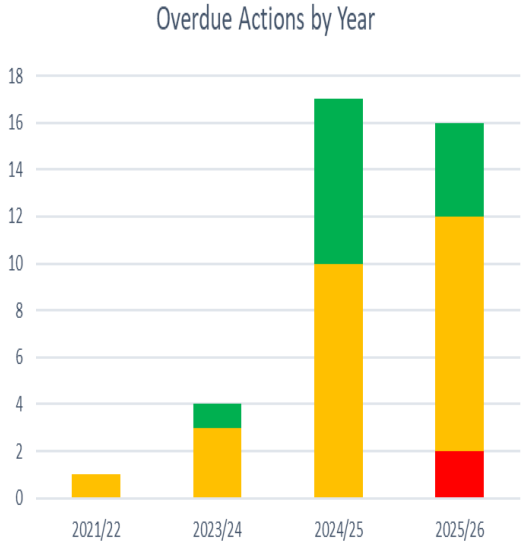
	The training comprehensively covered data breaches, however, it did not cover other areas outlined by the ICO. If staff are not appropriately trained on data breaches and information management in general, there is an increased risk of errors which may result in data breaches and mismanagement of information.
	Walkthroughs of the incident reporting process found that there was no documented procedure for decision making within the incident review process, such as RAG rating, decisions to report incidents to the ICO, decisions to investigate incidents or not, and decision to close incidents protected. This may result in inappropriate decisions made by those without authority.
	Through sample testing of incidents, a number of exceptions were noted regarding a lack of RAG rating, no evidence of reporting within 24 hours and evidence was also not retained to confirm closure of actions. Without evidence that reports are accurately RAG rated, reported and evidence retained to support closure of actions, we could not provide assurance that incidents were being managed as per the internal process.
	Sample testing also identified that the field for capturing lessons learnt was not consistently used for each incident. By not identifying lessons learnt, the root causes are not being addressed, and the same vulnerabilities remain.
	Several inconsistencies were found in the data captured on the incident management log, including missing fields, lack of classification, lack of RAG ratings and a number of 'open' status incidents from 2024. Additionally, there were inconsistencies between the number of incidents noted as being reported to the ICO on the incident management log and evidence folders maintained for the ICO reporting.
	Also, comparing the incident management log to best practice, the log does not include fields for capturing information on department/area of origin, location (physical or virtual), affected systems/assets, initial response, investigation, follow- up actions.

RECOMMENDATION ANALYSIS

Audit recommendations are made based on the level of risk posed by the weaknesses identified. The current ratings used are:



All recommendations are followed up on their due date and for any that have not been implemented the responsible officer can set a revised target date. Currently 38 recommendations are overdue based on their original target date. 26 of these are rated as medium or high.



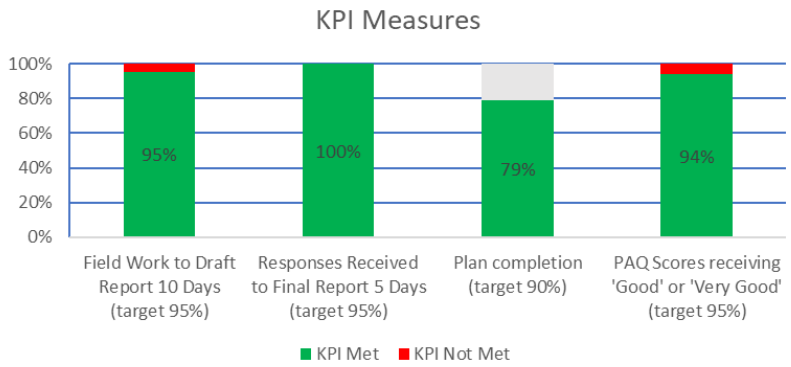
The overdue actions span across several years, and we continue to track those outstanding on a regular basis. Overdue recommendations are reported regularly into the Finance Governance Board, which is chaired by the Chief Finance Officer (OPCC). They are also regularly reported into the Commercial Services Governance Board chaired by the Director of Commercial and People Services (WMP) and on a quarterly basis, we provide updates to the relevant portfolio lead within the Force Executive Team.

An analysis of overdue recommendations by audit is provided at Appendix A, along with the latest progress update for any high and medium rated outstanding actions.

Of the recommendations followed up since 2021/22, 90% are considered implemented or redundant, with 10% still open.

Analysis of Recommendations									
	Made	Follow up Completed	Implemented		Open		Redundant/ Risk Accepted		Not Yet Followed Up
2021/22	106	106	99	93%	1	1%	6	6%	0
2022/23	84	84	67	80%	0	0%	17	20%	0
2023/24	72	72	65	90%	4	6%	3	4%	0
2024/25	89	88	70	80%	17	19%	1	1%	1
2025/26	93	40	24	60%	16	40%	0	0%	53
Total	**444**	**390**	**325**	83%	**38**	10%	**27**	7%	**54**

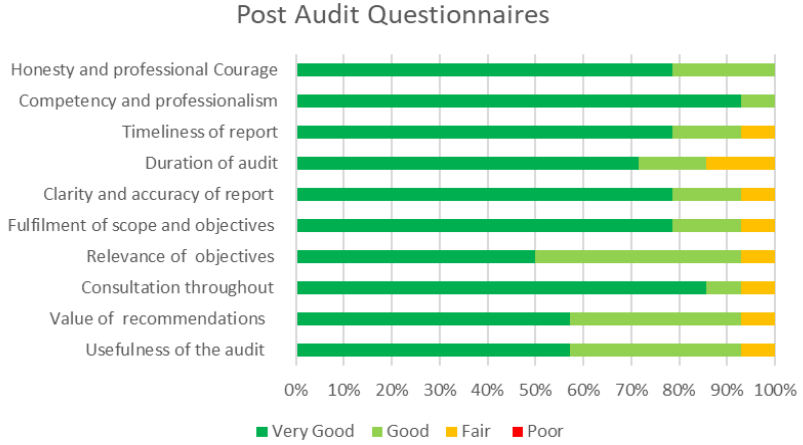
PERFORMANCE



The performance of internal audit is measured against a set of Key Performance Indicators. The latest is shown here.

The plan completion is currently on target, standing at 79%. A couple of amendments have been requested to the audit plan, which are discussed later in this report.

The reported position for issuing draft reports within 10 days of fieldwork end and for issuing final reports within 5 days following receipt of management responses are both on target.



Feedback on Post Audit Questionnaires is slightly below target with 94% of survey questions scored as ‘Good’ or ‘Very Good’. (Target 97%)

We have not received any feedback with a rating of poor.

100% of respondents agreed that the internal audit team understands their business area, its needs, objectives and risks. (Target 95%)

93% of respondents agreed that internal audit adds value. (Target 95%)

OTHER AREAS OF ACTIVITY

Our work on investigating the data matches from the 2024/25 National Fraud Initiative to identify any potential fraud or error is now complete. This exercise included payroll, pensions and creditor data that is matched against other public sector organisations.

A total of 65 deceased pensioner matches were identified, most of which were already known. Investigations identified £51,058 of overpayments to deceased pensioners which the Pensions Team are attempting to pursue with the relevant pensioner's estates.

With the cooperation of the Accounts Payable team, we also identified £186,795 creditor overpayments. This related to four creditor payments from the several hundred we investigated. The majority of this has been recovered.

CHANGES PROPOSED TO THE INTERNAL AUDIT PLAN

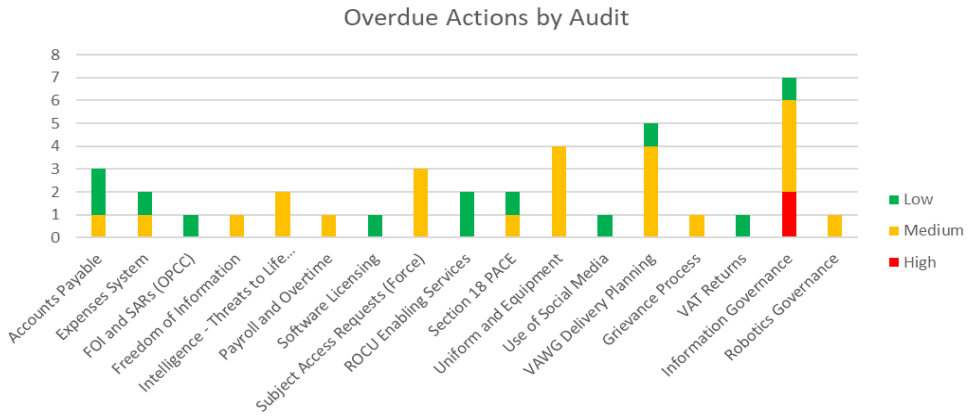
During the last reporting period, we received two requests to amend the audit plan. Both requests were made by the Force Executive Team and we consulted with the JAC Chair promptly to avoid unnecessary delay. The changes requested were as follows:

- Replace the planned audit of ROCU Serious and Organised Crime with a review of the Regional Economic Crime Unit.
  ROCU Serious and Organised Crime formed part of a recent HMICFRS inspection, and the Force are continuing their efforts to implement the actions arising. We were instead requested to utilise audit resource undertaking a review of the end-to-end processes within the Regional Economic Crime Unit (RECU). This unit has evolved over time with the most recent change being that Report Fraud has recently replaced Action Fraud for fraud reporting. Whilst Report Fraud is managed by City of London Police, this early review of the new arrangements will allow us to assess how the ROCU interacts with other Forces and City of London Police to manage fraud effectively. Due to the lateness of this request, we expect this to run into 2026/27 and have therefore included time for this in the 2026/27 audit plan.

- Postpone the review of Fleet Management.
  The Force recently commissioned external consultants to undertake a review of fleet management and the scope overlaps with a number of areas we planned to cover. The Force are currently awaiting the outcome of that review, so we were requested to postpone this audit for six to nine months to allow the Force to consider the outcomes and make any required improvements. We plan to undertake a review in the latter half of 2026/27 to consider progress to embed any changes and audit any residual aspects of fleet not covered by the external consultants review.

APPENDIX A – High/Medium Recommendations Outstanding after Follow-Up

This chart summarises the position of overdue recommendations by Audit. The table below the chart provides the latest updates for the 26 overdue recommendations currently rated as High or Medium.



Ref	Original Report to JAC	Audit	Recommendation	Target Date /Responsible Officer	Latest position based on responses provided by management
1	Sep -21	Accounts Payable	The scheduled task in regard to reconciliation of the BACS transmission file must be reinstated immediately. Following this, in conjunction with IT & Digital, steps should be taken to secure the BACS transmission file when being extracted from Oracle Fusion. This should include the file produced being read-only and being automatically transferred to the relevant network drive for upload to the bank.	*31 December 2021* *Head of Purchase to Pay*	Update January 2026 Still awaiting implementation date from bank.
2	Sep-23	Expenses System	To ensure that officers and staff claim Expenses correctly and use other purchasing processes appropriately: • Line Managers should be reminded of their responsibility to undertake detailed checks on expenses claimed prior to approval to ensure they are in accordance with Force policy, include all necessary information, are correct and that appropriate VAT receipts are attached when required. • They should also be reminded and encouraged not to approve items through the expenses system that should be processed through other purchasing processes i.e. through purchase orders on the Procurement system, via the NUMS Contract or via Occupational Health. Payroll team should periodically review the number and type of policy violations over a period of time with the aim of assessing reasons and communicating lessons learnt via a	*Assistant Director Finance, Contracts and Procurement & Head of Payroll* *(Revised to 31/3/26)*	Update January 2026 The policy has completed the consultation. We will need to tie up a few loose ends before it is signed off. Therefore, I expect a go live by the end of March.

Ref	Original Report to JAC	Audit	Recommendation	Target Date /Responsible Officer	Latest position based on responses provided by management
			suitable platform such as a message of the day article or via an update on the My Service Portal to help ensure that officers and staff use the Expenses system correctly and prevent further policy violations.		
3	Mar-24	Freedom of Information	The Force should ensure that a Data Breach Policy is adopted that clearly outlines the steps to follow if a breach were to occur. This policy should be made available to all employees.	*Civil Disclosure Unit Manager* *(Revised to 31/3/26)*	Update February 2026 Policy needs to be split into policy then process guidance, then EQIA template needs completing. Anticipating completion by 31/03/2026.
4	Mar-24	Payroll and Overtime	To maximise efficiency, opportunities to further develop the Overtime App should be explored including, for example, embedding supervision hierarchy, and preventing duplicate claims being submitted, therefore reducing the need for extensive checks conducted by Payroll and Finance.	*AD of Finance and* *Head of Payroll* *(Revised to 1/4/26)*	Update February 2026 The overtime app has been developed further, and user acceptance testing is underway with a view to phase 1 going live by April 2026.
5	Dec-24	Subject Access Requests (Force)	To maximise use of resources whilst improving engagement and communication with the person making a Subject Access Request (SAR), the CDU Manager should: • instruct Civil Disclosure Officers not to work on SAR's until the required identification documents are received; and • review the arrangements for managing and responding to correspondence relating to SAR's, removing the risk of single point of failure in the process and ensure prompt communication throughout the process.	*CDU Manager* *31/10/24* *(Revised to 01/04/26)*	Update December 2025 Work is on-going with Single Online Home and CYC 3 - There is still no update in relation to auto acknowledgements and whether it will be the set process moving forward. However, the team do not process any SARs without the correct ID. There is a workflow on the new CYC where we can select ID Unacceptable/Place files on hold where further information is required.
6	Dec-24	Subject Access Requests (Force)	To ensure reporting is accurate the Head of CDU should: • explore the reporting capabilities with suppliers of Cyc Freedom during the forthcoming upgrade to ensure that it meets the reporting requirement of CDU • ensure new SARs received are entered into Cyc Freedom promptly following receipt to make certain they are captured within the performance data reported • the cut-off date for compiling figures should be moved later in the month to accurately capture performance.	*CDU Manager* *31/12/24* *(Revised to 31/1/26)*	Update March 2026 The new Business Support Assistant (BSA) has not yet been recruited; however, the CDU supervisor is assisting with the mailbox to support the existing BSA
7	Dec-24	Subject Access Requests (Force)	The CDU Manager should restrict access to the Subject Access Review area of the Cyc Freedom to those that require it to perform their role.	*CDU Manager* *31/12/24* *(Revised to 21/7/25)*	Update December 2025 No further updates, the system won't be restricted to those who just do SARS as the vetting levels are the same.
8	Dec 24	Threats to Life	If a decision is made to formally adopt the revised National Threat to Life guidelines, this should be effectively communicated to all relevant staff to raise awareness of any significant change from the	*Chief Supt Intelligence*	Update January 2026

Ref	Original Report to JAC	Audit	Recommendation	Target Date /Responsible Officer	Latest position based on responses provided by management
			existing guidelines. Communication and awareness should particularly focus on those roles that could be responsible for managing a Threat to Life scenario who are not receiving formal training through the Senior Leaders Development Programme Hydra course.	*31/3/25* *(Revised to 31/3/26)*	A series of training videos are to be created and ready for publishing in the next two months – in the interim, the risk is being minimised as TTL oversight is still maintained in Force Intelligence by I24 on a 24/7 basis.
9	Dec 24	Threats to Life	The Intelligence department should produce a brief guide or publicity material on how to draft and deliver warning and disruption notices. The opportunity should also be taken to inform Officers of the range of support services they offer when drafting notices, and to prompt them to contact I24 when they are unsure or require advice.	*Chief Supt Intelligence* *31/03/2025* *(Revised to 31/03/26)*	Update January 2026 The video for front line officers has been delayed due to operational demands - ETA end of March. Advice on issuing TTL notices is being provided 24/7 from the I24 intelligence team who are all trained however it is still recognised that a video for front line officers would be beneficial. Two videos are planned - one for Officers and one for Inspectors writing notices
10	June 25	Section 18 PACE	To ensure compliance with Section 18 PACE, the Detective Chief Inspector (Op Vanguard) will: • provide further guidance on the circumstances when Section 18 PACE searches should be utilised by officers and where they should be recorded within Custody and Investigations records within Connect. • utilise newsbeat to further promote relevant guidance on officers' responsibility in ensuring robust record keeping for Section 18 PACE searches. • encourage compliance checks as part of Supervisor reviews to ensure appropriate records have been updated when Section 18 searches are performed and instances of non-compliance are addressed accordingly. The QAAT process will also be used to identify instances of non-compliance.	*Detective Chief Inspector* *(Revised to 30/4/26)*	Update March 2026 Further guidance has been provided in Initial Investigation Questionnaire set, and flow charts now displayed in Custody when a Section 18 should be considered. Initial Investigation template has been updated to prompt Supervisor review for Section 18. Promotion of relevance guidance is still outstanding. Op Vanguard have developed a blog and there will be a series of three. One has been issued on victims as this was the most important topic, and the other topics are Investigation and golden hours and suspects. The suspect blog will include details on use of Section 18 and where it should be recorded, this is likely to be issued in April 2026
11	June 25	Uniform & Equipment	As part of the implementation of the new HSO Uniform Ordering and Storage solution, a suite of reports or dashboards should be developed to inform and enable the various governance forums to undertake appropriate scrutiny of the uniform service and allow for improved decision making by management. This should include reporting on stock inventory, minimum/maximum stock levels required to meet demand, stock usage, trends, lost/missing stock, fulfilments time etc.	*Transport Logistics Manager* *(Revised to 30/4/26)*	Update March 2026 Linked to HSO roll out in April 2026. HSO system includes reporting on: Consumption by SKU Consumption by officer Demand by SKU Demand by officer Daily aggregates - no of picks, orders, average SKUs per order Coverage - weeks cover based on stock usage and held stocks. Stock exceptions - shows SKUs that are outside there set min/max stock levels Further reporting to be reviewed via Qlik once HSO is live
12	June 25	Uniform & Equipment	To strengthen and provide more consistent oversight of lost/missing items, records should be improved and include costs, type, location and officer to inform reporting into management and assist in identifying any patterns or trends arising that require further action. This should consider whether any reports should be provided to local Commanders, as well as governance boards.	*Transport Logistics Manager* *Revised to 30/4/26)*	Update March 2026 This is linked to the roll out of the HSO stock management system. This is due April 2026.

Ref	Original Report to JAC	Audit	Recommendation	Target Date /Responsible Officer	Latest position based on responses provided by management
13	June 25	Uniform & Equipment	To ensure a robust process is in operation for the return of uniform and equipment: • The WMP uniform return process within Frequently Asked Questions should provide guidance on the process to follow for both individuals and line managers when an employee leaves the Force. • Consider producing a standard list of personal issue uniform and equipment to support line managers recovering items, with particular emphasis on items that would identify an individual as a WMP Police employee. • Explore potential within the new HSO Uniform Ordering and Storage Solution to report on any sensitive, specialist or high value items of uniform and equipment to be recovered by line managers.	*Transport Logistics Manager* *(Revised to 30/4/26)*	Update October 2025 We are now notified of leavers. We send them via the My Service Portal instructions. This generates a reference number to allow tracking of items returned. This will be updated on the FAQ's on the Uniform Services intranet page. Bullets 2 & 3 - linked to deployment of HSO system in April 2026
14	June 25	Uniform & Equipment	To strengthen performance management arrangements, introduce a series of key performance indicators / service expectations to measure the performance of the internal Uniform and Stock management functions service, with results reported into the appropriate governance group at regular intervals.	*Transport Logistics Manager* *(Revised to 30/04/26)*	Update September 2025 This is dependent on the implementation of the HSO stock management system in order to provide accurate data for KPI's to be based on. The HSO system is currently due to go live at the start of April 2026
15	Sept 25	Grievance Process	The Employee Relations Manager will incorporate additional columns into the grievance tracker to capture appropriate detail relating to recommendations arising from grievances, including target date, responsible officer and progress update, and going forward the grievance will be kept updated with progress made on recommendations.	*Employee Relations Manager* *(Revised to 30/6/26)*	Update March 2026 As we have had a very limited number of formal grievances since the audit was performed, we are only now getting to the point of being able to evidence the newly introduced procedure with appropriate follow up to ensure actions identified are completed and learning is embedded.
16	March 26	Robotics Governance	The Mobility and Automation Manager and the CAA Steering Group chair will review the group meetings to ensure that they: • Meet at a defined frequency to monitor and oversee the ideas into the CAA team and progress of those in development/implementation. • Adopt minutes or decisions and actions logs to help ensure that decisions made by the group and transparent and recorded for future reference. • Adopt terms of refence for the group to formally set out the remit, membership, frequency, and outputs from the group.	*Head of Delivery Management* *31/12/25* *(Revised to 31/3/26)*	Update January 2026 The Terms of Reference for the CAA Steering Group are being revised following the new Head of Delivery Management taking over responsibility to chair the meetings. This is due to be completed by the end of March 2026.
17	Dec 25	Information Governance	The Force should review its suite of information management policies and guidance and ensure that these capture information in relation to the below, as expected by the Information Commissioner's Office: • Creating, locating and retrieving records • Security for transfers	*Data Protection and Information Lead* *01/02/26*	Update February 2026 Policy work is anticipated to be complete by 31/03/2026

Ref	Original Report to JAC	Audit	Recommendation	Target Date /Responsible Officer	Latest position based on responses provided by management
			• Destruction • Rules for acceptable software use • Access control • Unauthorised access • Mobile devices, home or remote working and removable media • Secure areas Once reviewed and signed off by the Chief Constable, the policies should be maintained on the intranet for access by staff.	*(Revised to 31/3/26)*	
18	Dec 25	Information Governance	The Force should develop an Information Management Strategy in place to outline the structured approach to organising, storing, accessing, and protecting data and information assets to ensure they are efficiently utilised to support decision-making, enhance productivity, and align with the Force's objectives and compliance requirements.	*Data Protection and Information Lead* *01/02/2026* *(Revised to 31/3/26)*	Update February 2026 Information Management strategy is in progress and is anticipated to be complete by 31/03/2026
19	Dec 25	Information Governance	The Force should ensure that incidents are RAG rated timely, a clear record is maintained for the notification of red and amber incidents to the Data Protection officer and Head of Information Security. Records should be consistently maintained to evidence action taken to support the closure of incidents.	*Data Protection and Information Lead* *01/12/2025*	Update February 2026 Waiting for new workers to start in IT&D as we need SharePoint expertise for this.
20	Dec 25	Information Governance	The Force should ensure: - all fields within the incident management log are populated timely to enable to the log to reflect the most complete and up to date information. - the log accurately reflects the incidents reported to the Information Commissioner's Office (ICO) and that there is a reference/link between the evidence maintained for reporting to ICO and information captured on the incident management log for monitoring and reconciliations. - incidents are closed timely, and the status is accurately reflected in the incident management log. This will enable reliance on the information captured on the log and reported on.	*Data Protection and Information Lead* *31/12/2025*	Update February 2026 Waiting for new workers to start in IT&D as we need SharePoint expertise for this.
21	Dec 25	Information Governance	The Force should update the incident management log to capture details of department/area of origin, location (physical or virtual), affected systems/assets, initial response, investigation, follow-up actions (i.e. monitoring, training, audits)	*Data Protection and Information Lead* *31/12/2025*	Update February 2026 Waiting for new workers to start in IT&D as we need SharePoint expertise for this.

Ref	Original Report to JAC	Audit	Recommendation	Target Date /Responsible Officer	Latest position based on responses provided by management
22	Dec 25	Information Governance	The Force should ensure that the tracker for Information Commissioner's Office recommendations is kept up to date, outstanding actions are assigned a due date and responsible owner for monitoring and effective implementation. Where recommendations are confirmed as completed by the Commissioner, the Force should ensure that the actions and improvements are maintained to avoid the same issues being raised by the ICO.	*Data Protection and Information Lead* *31/12/2025*	Update February 2026 Waiting for new workers to start in IT&D as we need SharePoint expertise for this.
23	Sept 25	VAWG Delivery Planning	The VAWG lead will ensure that appropriate records are maintained for the relevant board/delivery group meetings to evidence that delivery plans are reviewed, with further action, approvals or decisions being clearly recorded e.g., when actions are agreed for closure by the board/group.	*VAWG lead* *30/11/2025* *(Revised to 31/3/26)*	Update March 2026 The delivery plan is being revised to incorporate actions from the new Government VAWG strategy, the WMP VAWG Problem Profile and the Angiolini 2 Recommendations. The delivery plan will be hosted on the VAWG teams channel so it can be updated by strand leads and it will be monitored through the VAWG Steering Group. Administrative support is provided through the PPU PA. Delivery plan should be ready by end of March 2026.
24	Sept 25	VAWG Delivery Planning	The VAWG lead will ensure that delivery plans are in place for all VAWG strands and that these, along with the WMP VAWG Pledges tracker, are reviewed at relevant meetings and updated regularly. Target completion dates are to be included in the plans so that any slow progress or items requiring escalation to senior management can be identified and actioned.	*VAWG lead* *30/11/2025* *(Revised to 31/1/26)*	Update March 2026 The delivery plan is being revised to incorporate actions from the new Government VAWG strategy, the WMP VAWG Problem Profile and the Angiolini 2 Recommendations. The delivery plan will be hosted on the VAWG teams channel so it can be updated by strand leads and it will be monitored through the VAWG Steering Group. Administrative support is provided through the PPU PA. Delivery plan should be ready by end of March 2026.
25	Sept 25	VAWG Delivery Planning	Reporting progress on the VAWG delivery plan and those supporting the overall VAWG delivery plan e.g., Safer Spaces, RASSO, DA etc. will be reviewed by the VAWG Lead to ensure regularly reporting into the appropriate group/board meetings.	*VAWG lead* *30/11/2025* *(Revised to 31/1/26)*	Update March 2026 The Terms of Reference have been rewritten, and the delivery plan is being revised to incorporate actions from the new Government VAWG strategy, the WMP VAWG Problem Profile and the Angiolini 2 Recommendations. The delivery plan will be hosted on the VAWG teams channel so it can be updated by strand leads and it will be monitored through the VAWG Steering Group. Administrative support is provided through the PPU PA. Delivery plan should be ready by end of March 2026.
26	Sept 25	VAWG Delivery Planning	The VAWG Lead will assess the coverage of the Force's Vulnerability performance management framework to identify and adopt any further VAWG specific performance measures to support delivery of the VAWG Strategy ambitions.	*VAWG lead* *30/11/2025* *(Revised to 31/1/26)*	Update March 2026 The delivery plan is being revised to incorporate actions from the new Government VAWG strategy, the WMP VAWG Problem Profile and the Angiolini 2 Recommendations. The delivery plan will be hosted on the VAWG teams channel so it can be updated by strand leads and it will be monitored through the VAWG Steering Group. Administrative support is provided through the PPU PA. Delivery plan should be ready by end of March 2026.