



west midlands  
police and crime  
commissioner



# INTERNAL AUDIT ACTIVITY REPORT

**Joint Audit Committee**  
**25 June 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 March 2026 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.

<b>CONTACT OFFICER</b>
------------------------

Name: Lynn Joyce
------------------

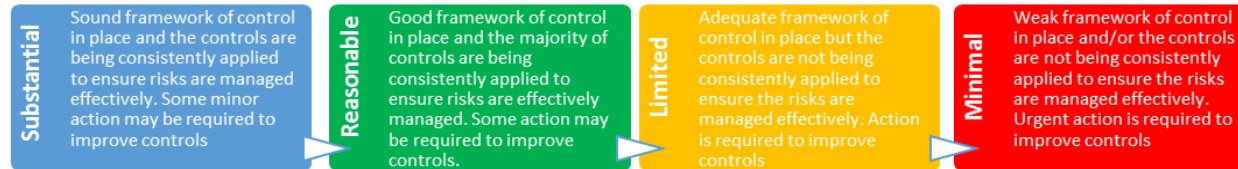
Title: Head of Internal Audit
-------------------------------

<b>BACKGROUND DOCUMENTS</b>
-----------------------------

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:



This audit update report covers the latter part of 2025/26 and the start of 2026/27.

- Table 1 below captures those audits completed to final stage in 2025/26, along with their opinions, which have been used to form the Head of Internal Audit conclusion, reported separately.
- Table 2 includes those 2025/26 audits that were not completed to final stage by year end which have been carried forward to 2026/27, along with the audit plan for 2026/27. The 2026/27 audit plan is in its infancy and will continue to be populated as audits progress.

Four audit reports were finalised during the reporting period, one of which received a Limited opinion. Four audit reports are currently in draft awaiting management comments. The pages that follow summarise those audits that received minimal or limited assurance.

**Table 1- Audits completed to final stage in 2025/26**

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
Central Ticketing Office	Final	Minimal
Cyber Security	Final*	Reasonable
Force Contact Resourcing	Final*	Reasonable
Contingent Workers	Final*	Limited
Benefits Realisation	Final*	Reasonable
Social Media Strategy	Final	Reasonable

Audit	Status	Opinion
Grievance Process	Final	Reasonable
Robotics Governance	Final	Reasonable
Gifts and Hospitality (OPCC)	Final	Reasonable
Gifts and Hospitality (Force)	Final	Reasonable
Cash Office Functions	Final	Reasonable
Bank Reconciliation	Final	Substantial
VAT	Final	Substantial
Risk Management	Final	Substantial
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

\*Finalised during reporting quarter

**Table 2 - 2026/27 Audit Plan**

Audit	Status	Opinion
<b>2025/26 Audits in progress at year end brought forward to 2026/27</b>		
Civil Contingencies	Draft	
Records Management /Compliance with MOPI	Draft	
Income Generation – Driver Improvement Courses	In progress	
Forensic Medical Statements	Draft	
Payroll	Draft	
<b>2026/27 Audit Plan</b>		
Budgetary Controls and MTFP		
Debtors	In progress	
Expenses and Allowances		
Income Generation		
Detained Property		
Occupational Health		
HR Admin Functions	Planning	
MS365 Governance		
AI Governance		
Information and Records Management		
Information Sharing agreements		
Fleet Management		
Neighbourhood Policing Guarantee		
LPA Governance, Data and Performance Management - Birmingham		
Regional Economic Crime Unit	Planning	
Right Care Right Person		
MARAC Governance and Co-ordination	In progress	
Sex Offender Management		
Drones Unit		
Diversity, Equality and Inclusion Strategy	Planning	

Audit	Status	Opinion
ANPR Capability		
Force Contact - Crime Desk	In progress	
Force Governance and Business Planning Arrangements		
Service Recovery/complaints		
Equality Impact Assessments		
Complaints, Reviews and Organisational Learning		

*\*Finalised during reporting quarter*

## LIMITED OPINION AUDIT – Contingent Workers

### Objectives and Scope

This review focused on the effectiveness of the Force’s management, classification and oversight of contingent workers to mitigate the associated risks. The areas reviewed included:

- Governance and performance monitoring arrangements, including policies and procedures, reporting lines, oversight responsibilities and reporting arrangements.
- Compliance with legal duty requirements and procurement regulations, including record keeping to demonstrate adherence to contract standing orders.
- Processing arrangements, including controls around verifying and processing contingent workers, i.e., accurate and timely processing of starters, leavers, up to date vetting and access controls etc.

### Overall Opinion



**LIMITED ASSURANCE**

*(Definitions of ratings are provided at Appendix A)*

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.

### Number of Actions

High	0
Medium	5
Low	1
Total	<b>6</b>

### Conclusion

A risk was recorded on the Force risk register in 2023 regarding contingent workers remaining active on police systems after leaving. Remedial work followed to remove a number of contingent workers with expired vetting or who had not accessed premises over the past 12 months, and the risk was subsequently closed. However, since this remedial work was completed, there has been no routine monitoring and records continue to be out of date. We found examples of system and/or premises access not being removed promptly following the contingent worker leaving, and locally maintained records were often insufficient to provide assurance that contingent workers are properly managed.

These weaknesses are reflected in the limited opinion and we propose that the original risk is reopened until processes are strengthened.

The opinion also reflects a breach of Contract Standing Orders which was identified and corrected by Contracts and Procurement prior to the audit commencing.

### Good Practice

- All new contingent workers are required to complete the College of Policing College Learn module 'Managing information' training prior to them gaining access to the corporate network which we confirmed via sample testing. This ensures contingent workers understand their responsibility around information security and data protection when working for the Force.

### Key Findings Summary

Contingent workers usage is not analysed to identify instances of over utilisation or prolonged reliance etc, and no information is currently reported into governance boards to assess the appropriateness of contingent workforce use.

Corporate Asset Management (CAM) and other business areas maintain a contractors database which is accessible to all staff and officers for the purpose of confirming contractors' details and vetting is suitable, however, this database is not being updated routinely resulting in incomplete or out of date information. This presents a risk that a contractor may inappropriately be granted access to a police building.

Local records of contingent workers within IT & Digital have not been routinely updated for some time and therefore do not accurately reflect the contingent workers engaged. This creates potential for reduced management oversight of the contingent workforce within this business area.

Vetting Single Points of Contacts (SPOCs) have been assigned within each business area who hold responsibility for co-ordinating the vetting of contingent workers. Line Managers often fail to notify their Vetting SPOC when a contingent worker leaves and, as a result, examples were identified of system access and access to buildings not being removed promptly.

The Force use two separate systems for managing vetting and access for contingent workers. Vetting is processed and recorded in Core-Vet, and access to systems and buildings is managed through Oracle Fusion. No periodic reconciliation is performed between these systems to confirm data accuracy, and data analytics undertaken during the audit identified

## LIMITED OPINION AUDIT – Contingent Workers (Continued)

discrepancies between the data sets. This further increases the risk of contingent workers retaining inappropriate access to systems and buildings.

IR35 determines whether a contingent worker employed through a company should be treated as an employee for tax purposes. Finance performs the assessment on determination of IR35, however no formal guidance is provided to departments on how to raise concerns or seek further advice regarding IR35 determinations. This can lead to staff working inconsistently and increase potential for a lack of compliance with the agreed approach.

## OTHER AREAS OF ACTIVITY

Investigations into the data matches from the 2024/25 National Fraud Initiative have concluded, with preparations now underway for the data submission for the 2026/27 exercise. We plan to undertake trial data extracts over the summer months in preparation for data submission in October 2026. This data submission will include payroll, pension and creditor data which the Cabinet Office will match against other public sector organisations.

Regarding the 2024/25 exercise, the investigations yielded total outcomes of £237,854:

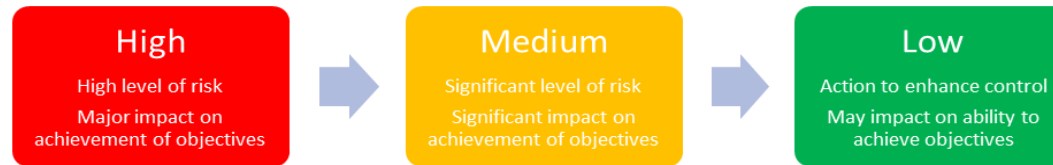
- A total of 65 deceased pensioner matches were identified, most of which were already known. Investigations identified £51,058 of overpayments to deceased pensioners which the Pensions Team are attempting to pursue with the relevant pensioner's estates.
- With the cooperation of the Accounts Payable team, we also identified £186,796 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

There have been no new audit requests during the reporting period and no changes to the proposed plan.

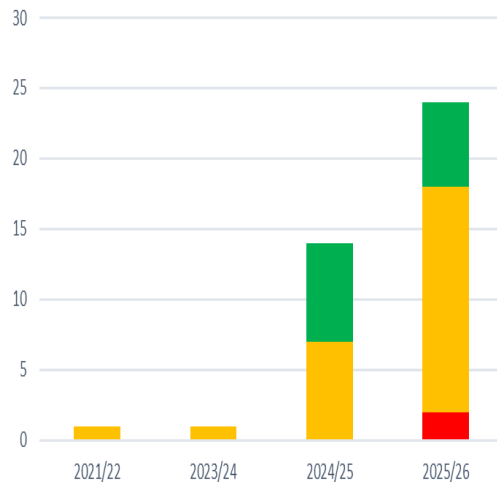
## RECOMMENDATION ANALYSIS

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 45 recommendations are overdue based on their original target date, of which 31 are rated as medium or high.

Overdue Actions by Year



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.

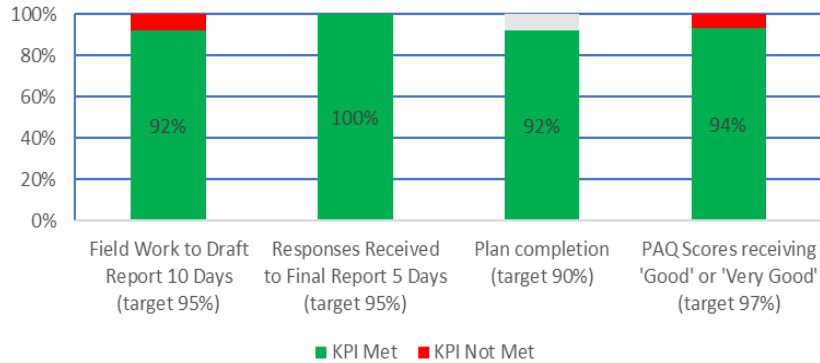
An analysis of overdue recommendations by audit is provided at Appendix A, along with the latest progress update for any high and medium rated outstanding actions.

Of the recommendations followed up since 2021/22, 90% are implemented or redundant.

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	67	93%	1	1%	4	6%	0
2024/25	89	89	75	84%	13	15%	1	1%	0
2025/26	113	77	47	61%	30	39%	0	0%	36
<b>Total</b>	<b>464</b>	<b>428</b>	<b>355</b>	<b>83%</b>	<b>45</b>	<b>11%</b>	<b>28</b>	<b>7%</b>	<b>36</b>

## PERFORMANCE

KPI Measures

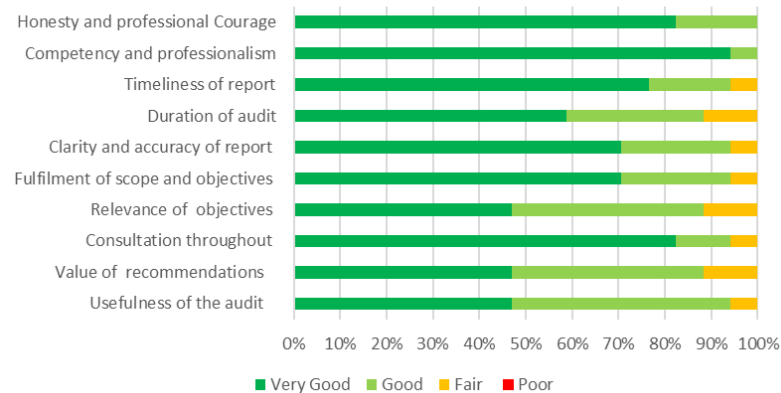


The performance of internal audit is measured against a set of Key Performance Indicators. The 2025/26 year-end position on progress is shown here. It is currently too early to measure 2026/27 performance as we are working on completing the last few audits from 2025/26 and the audits for 2026/27 are in early stages of the audit process.

The plan completion for 2025/26 was 92% against a 90% target. We have now progressed all but one of the 2025/26 audits to draft report stage.

The reported position for issuing draft reports within 10 days of fieldwork end came in below target at 92% against a target of 95%, with two audits failing to meet the 10-day target. The target for issuing final reports within 5 days following receipt of management was met.

Post Audit Questionnaires



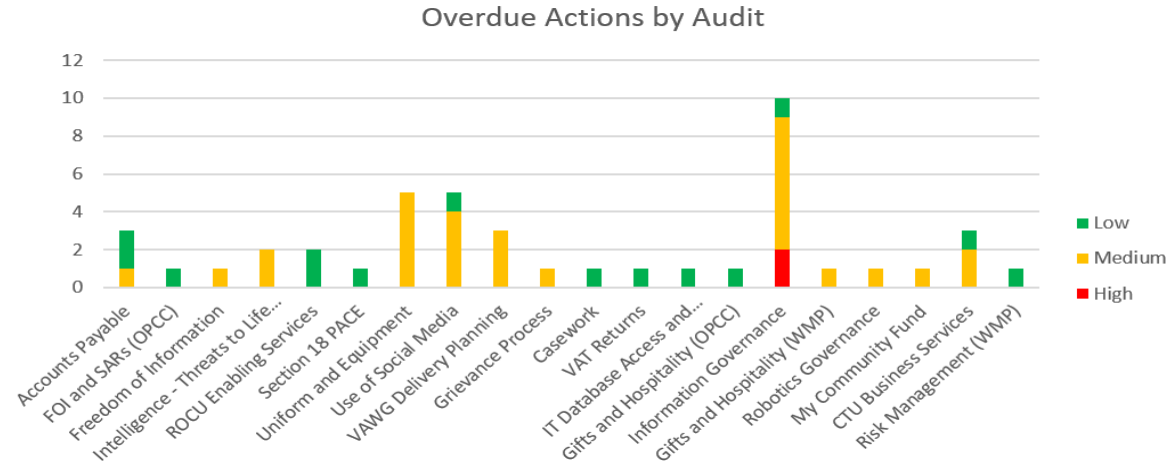
Feedback on Post Audit Questionnaires was slightly below target with 94% of survey questions scored as 'Good' or 'Very Good' (Target 97%). We have not received any feedback with a rating of poor.

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

94% of respondents agreed that internal audit adds value (Target 95%).

## 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 31 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.	<i>Head of Purchase to Pay</i> 31/12/21	<u>Update May 2026</u>  A meeting with IT and the NatWest Implementation Manager was held 20/5/26. This process is due to commence mid-June and will take approximately 3 months to be implemented. From June 1st weekly meetings are due to start with all parties involved, to keep this on track.  BACS Transmission Reconciliations continue to be carried out (by Supplier Management) after each Supplier Payment run. This will continue until the new automated process is in place.
2	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.	<i>Civil Disclosure Unit Manager</i>  (Revised to 10/6/26)	<u>Update June 2026</u>  The draft policy has been updated and EQIA will be completed by 10/06/2026.
3	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 existing guidelines. Communication and awareness should particularly focus on those roles that could be responsible for	<i>Chief Supt Intelligence</i> 31/3/25	<u>Update June 2026</u>  Briefings into teams have been delivered. The change to Policy is yet to be actioned – options will be considered and presented to Exec (either maintain

Ref	Original Report to JAC	Audit	Recommendation	Target Date /Responsible Officer	Latest position based on responses provided by management
			managing a Threat to Life scenario who are not receiving formal training through the Senior Leaders Development Programme Hydra course.	(Revised to 31/3/26)	current status quo and accept that sits outside of national guidance, or a force policy change and for review by Supt in line with national guidance).
4	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)	<u>Update June 2026</u>  Briefings into teams have been delivered. The change to Policy is yet to be actioned – options will be considered and presented to Exec (either maintain current status quo and accept that sits outside of national guidance, or a force policy change and for review by Supt in line with national guidance).
5	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 30/6/26)	<u>Update May 2026</u>  A small number of reports have been created but as yet there is no information to populate them as the new system has not yet been implemented. Once the system is in place we will be able to see what information we can get from it and produce further reports as required.  HSO testing is complete and approval for ongoing maintenance contract was agreed at Change Board. New maintenance contract (3 years) agreed at May CRAB. Contract sent to HSO for signature. Once in place IT&D CAB will look to approve go live for June 2026.
6	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)	<u>Update May 2026</u>  Action to be taken is linked to the roll out of HSO, which now has an expected go live date of June 26.
7	June 25	Uniform & Equipment	To ensure a robust process is in operation for the return of uniform and equipment:  <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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.</li> </ul>	Transport Logistics Manager  (Revised to 30/6/26)	<u>Update May 2026</u>  Further development work once HSO live and working with Off boarding to ensure a robust process.  <i>Internal Audit note – Bullet 1 has been addressed FAQs now provide information on the leavers process. Bullets 2 &amp; 3 are linked to deployment of HSO system, due in June 2026</i>

Ref	Original Report to JAC	Audit	Recommendation	Target Date /Responsible Officer	Latest position based on responses provided by management
8	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.	<i>Transport Logistics Manager</i>  (Revised to 30/06/26)	<u>Update May 2026</u>  HSO go live due June 2026. KPI's have been discussed in Accountability Board. Awaiting implementation of HSO to fully understand what the capabilities of the system are.
9	June 25	Uniform & Equipment	To enable an accurate stock position to be available and to minimise the risk of misappropriation, a stock take schedule should be devised that considers: <ul style="list-style-type: none"> <li>• frequency - with all items being checked at least once a year, more frequently for higher value stock</li> <li>• verification – with actual stocks being verified to expected stocks</li> <li>• record keeping and evidence requirements - to support who undertook the check, findings and any investigation where discrepancies arise.</li> </ul>	<i>Transport Logistics Manager</i>  31/03/26  (Revised to 30/06/26)	<u>Update May 2026</u>  End of year stock take completed for 2025/26. Rolling stock take to be initiated once HSO system live.
10	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.	<i>Employee Relations Manager</i>  (Revised to 31/10/26)	<u>Update June 2026</u>  We now have 4 grievance meetings, and 3 grievance appeals in the current year which have been entered on the lessons learnt section of the grievance spreadsheet and have allocated officers for implementation and tracking of the lessons learnt. I have extended the date to allow this to be followed through to ensure the new process is working.
11	March 26	Robotics Governance	To enhance transparency of the hypercare and maintenance of RPA following go live: <ul style="list-style-type: none"> <li>• The relevancy and contents of the technical document will be reviewed and decision taken as to whether it should be used for all robots and whether the contents of the documents are covering sufficient detail. The Technical Support document will be reviewed with possibility to be extended to include the hypercare offer agreed with the business leads, e.g., meeting, performance monitoring, and any other specific asks, such as the business leads informing the CAA team and ensuring that robots are included in the departmental business continuity plans where required.</li> <li>• The CAA Steering Group chair and the Mobility and Automation Manager will also agree arrangements with the CAB chair for notification of upcoming upgrades or patches on systems with live RPA so that the CAA team can monitor and prepare for any impact robotic activity</li> </ul>	<i>Mobility &amp; Automation Manager and Head of Delivery Management</i>  31/3/26  (Revised to 30/9/26)	<u>Update June 2026</u>  New roles profiles submitted to HR for creation and establishment uplift to create the dedicate resource for post-hypercare support.
12	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: <ul style="list-style-type: none"> <li>• Creating, locating and retrieving records</li> </ul>	<i>Data Protection and Information Lead</i>  01/02/26	<u>Update June 2026</u>  The policy work will be completed by 19/07/2026; contractors are reviewing them as part of ICO audit.

Ref	Original Report to JAC	Audit	Recommendation	Target Date /Responsible Officer	Latest position based on responses provided by management
			<ul style="list-style-type: none"> <li>• Security for transfers</li> <li>• Destruction</li> <li>• Rules for acceptable software use</li> <li>• Access control</li> <li>• Unauthorised access</li> <li>• Mobile devices, home or remote working and removable media</li> <li>• Secure areas</li> </ul> <p>Once reviewed and signed off by the Chief Constable, the policies should be maintained on the intranet for access by staff.</p>	(Revised to 19/7/26)	
13	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 19/7/26)	<u>Update June 2026</u> The policy work will be completed by 19/07/2026; contractors are reviewing them as part of ICO audit.
14	Dec 25	Information Governance	The Force should ensure that information management policies and procedures are updated to clearly outline the roles and responsibilities of all staff ensuring that staff understand their duties and importance of their role in maintaining data integrity and security.	Data Protection and Information Lead 31/03/2026 (Revised to 19/7/26)	<u>Update June 2026</u> Policies are being reviewed and updated. This work will be completed by 19/07/2026.
15	Dec 25	Information Governance	The Force should consider establishing processes for regular escalation of non-compliance with information management training outside of the Performance Day.	Data Protection and Information Lead 31/03/2026 (Revised to 30/10/26)	<u>Update June 2026</u> The new DP training will go live in Oct 2026 on the new Learning Management System.
16	Dec 25	Information Governance	The Force should include annual training to encompass other key areas of data protection and information governance training in addition to data breaches, such as handling requests, data sharing, information security, and records management.	Data Protection and Information Lead 01/02/2026 (Revised to 30/10/26)	<u>Update June 2026</u> This is on track to be delivered in Oct 2026.
17	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.	Data Protection and Information Lead 01/12/2025	<u>Update June 2026</u> System requirements have gone into IT&D.

Ref	Original Report to JAC	Audit	Recommendation	Target Date /Responsible Officer	Latest position based on responses provided by management
			Records should be consistently maintained to evidence action taken to support the closure of incidents.		
18	Dec 25	Information Governance	<p>The Force should ensure:</p> <ul style="list-style-type: none"> <li>- 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.</li> <li>- 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.</li> <li>- incidents are closed timely, and the status is accurately reflected in the incident management log.</li> </ul> <p>This will enable reliance on the information captured on the log and reported on.</p>	<p><i>Data Protection and Information Lead</i></p> <p>31/12/2025</p>	<p><u>Update June 2026</u></p> <p>System requirements have gone into IT&amp;D.</p>
19	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)	<p><i>Data Protection and Information Lead</i></p> <p>31/12/2025</p>	<p><u>Update June 2026</u></p> <p>System requirements have gone into IT&amp;D.</p>
20	Dec 25	Information Governance	<p>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.</p> <p>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.</p>	<p><i>Data Protection and Information Lead</i></p> <p>31/12/2025</p>	<p><u>Update June 2026</u></p> <p>System requirements have gone into IT&amp;D.</p>
21	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.	<p><i>VAWG lead</i></p> <p>30/11/2025 (Revised to 31/5/26)</p>	<p><u>Update April 2026</u></p> <p>The draft delivery plan is due to be presented at the VAWG Steering Group at the end of April for sign off and will then be tracked through the steering group thereafter.</p>
22	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.	<p><i>VAWG lead</i></p> <p>30/11/2025 (Revised to 31/5/26)</p>	<p><u>Update April 2026</u></p> <p>A redrafted delivery plan will be presented to the next VAWG steering group at the end of April for sign-off. It will then go live and be tracked through VAWG steering group. It includes some elements of the new Government VAWG strategy, Angiolini 2 and the recommendations from the latest WMP VAWG problem profile. What it will not cover are where there are existing</p>

Ref	Original Report to JAC	Audit	Recommendation	Target Date /Responsible Officer	Latest position based on responses provided by management
					plans in place which are managed under other governance streams such as the DA Delivery Plan and Op Soteria Delivery Plan.
23	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 31/5/26)	<u>Update April 2026</u>  The new VAWG delivery plan should be launched by the end of April. Other delivery plans such as DA, RASSO are monitored through Vulnerability Improvement Board so that will not be duplicated through VAWG Steering Group. However, with the refreshed Terms of Reference for VAWG Steering Group, DCIs from those other areas are represented and there is the opportunity to task across for those strands if any gaps are identified.
24	Sept 25	Use of Social Media	CCD SLT will ensure that social media accounts accessed outside of Orlo are assigned to relevant staff/officers once the social media accounts review is completed, following which methodology for periodically reviewing users will be established to ensure that central records of social media accounts and users are accurate and up to date and allows for prompt removal of access that's no longer required.	Head of News 31/12/25 (Revised to 11/9/26)	<u>Update June 2026</u>  Our previous review and audit were completed in February 2025 / 2026. We are now undertaking a new cybersecurity review, which will include updating the current user list, enforcing password changes, and ensuring that email addresses are correctly aligned to centralised neighbourhood accounts. From this year onward, social media audits will take place twice annually.
25	Sept 25	Use of Social Media	CCD SLT will adopt a process to monitor posts and comments on social media accounts that are currently not monitored and responded to by the Digital Desk. Whilst a solution is being explored, management will consider if interim checks could be achieved through dip sampling to help ensure that requests and queries from members of the public are responded to promptly.	Head of News 31/12/25	<u>Update June 2026</u>  We have introduced new AI enabled moderation tools within Orlo. These tools automatically triage incoming messages and social media comments into categories such as actionable calls for service, intelligence, engagement, offensive content, and trust and confidence. This upgrade has already strengthened our monitoring capability, improved responsiveness to the public, and enhanced our ability to manage information disorder and identify recurring themes and issues. Messages are monitored by CCD during core office hours and Digital Desk 24/7 including on call and out of hours.
26	Sept 25	Use of Social Media	CCD SLT will assess the feasibility of recording potential breaches of policy, issues of compliance with code of conduct etc. in the use of social media that are identified from the social media content monitoring that CCD undertake and agree the criteria for reporting issues identified. A summary of issues will then be incorporated into existing governance reports to inform wider learning.	Head of News 31/12/25	<u>Update June 2026</u>  The Digital Production and Content Manager will log all social media breaches in a spreadsheet managed by the Digital Team. CCD will use this data to support future policy development and training requirements.
27	Sept 25	Use of Social Media	Following the ongoing review to assess current social media accounts that are in use and whether they are needed, CCD SLT will adopt timescales to complete the process of closing or moving accounts to Orlo and a target number of accounts (which may be based on the number of Orlo licences and thereby need to assess cost implications).	Head of News 31/12/25 (Revised to 31/12/26)	<u>Update June 2026</u>  As part of the review, we will identify inactive accounts and begin phasing them out. We are currently assessing alternative platforms for officers to share hyperlocal updates, including WMNow and Viva Engage. We want to avoid closing accounts prematurely and risking a decline in morale among our most active contributors, so we will wait until we can confidently offer a suitable alternative. Our target is to phase out Neighbourhood X accounts by December 2026 and transition users to other channels such as Orlo and WMNow.

Ref	Original Report to JAC	Audit	Recommendation	Target Date /Responsible Officer	Latest position based on responses provided by management
28	Dec 25	Gifts and Hospitality (WMP)	<p>The Detective Chief Inspector for Prevention and Intervention will:</p> <ul style="list-style-type: none"> <li>- Redesign the monthly gifts and hospitality return (WG450) to ensure it incorporates all relevant details, i.e., rationale for decision making, approval by decision makers (LPA standards Managers), circumstance of offer. The redesigned form should be accompanied by clear guidance for staff on how to complete the form and the level of detail required.</li> <li>- Develop formal training for decision makers, covering policy requirements, approval thresholds, escalation procedures and record keeping expectations.</li> <li>- Review the gifts and hospitality register prior to publication to verify completeness, accuracy and to prevent erroneous entries.</li> </ul>	<p><i>Detective Chief Inspector PSD Senior Investigation Manager</i></p> <p>31/5/26 (Revised to 30/5/26)</p>	<p><u>Update May 2026</u></p> <p>Revised target date proposed to allow for a number of meetings scheduled to take place</p>
29	March 26	My Community Fund	<p>The OPCC will establish a new 'one-time payment' process to allow for more timely payments to grant recipients. To establish a robust process, the OPCC will:</p> <ul style="list-style-type: none"> <li>- Design and/or adopt an existing standard operating procedure to verify recipient bank details. Evidence of verification of supplier bank details should be retained for all recipients receiving grant funds.</li> <li>- Devise a standardised payment request form that will be utilised for all MCF payments, this form should be forwarded directly to P2P to process once complete.</li> <li>- Ensure the form captures all required information, such as the recipient's name, contact details, full bank details and purpose of payment. The Form should include a section for a secondary staff member that is different to the requestor to authorise and verify the payment request.</li> </ul>	<p><i>Commissioning Advisor (OPCC)</i></p> <p>31/3/26 (Revised to 31/5/26)</p>	<p><u>Update April 2026</u></p> <p>The form has been prepared, but the process is not tested yet.</p>
30	March 26	CTU Business Services	<p>The Deputy Head of Business Services, in consultation with the Head of Business Services, will take the following steps to improve transparency of reporting:</p> <ul style="list-style-type: none"> <li>• Review the Service Delivery Framework to clearly identify performance indicators for each service area, as opposed to a record of activity delivered.</li> <li>• Where possible, targets will be adopted for each KPI agreed and approved appropriately by SLT/governance board to ensure transparency of acceptable performance.</li> <li>• Performance will be reported by month and on a cumulative basis to enable a true picture of any outstanding work to be reported upon.</li> <li>• Performance reported will be supported by commentary, if not on target.</li> </ul>	<p><i>Deputy Head of Business Services</i></p> <p>1/4/26 (Revised to 30/4/26)</p>	<p><u>Update May 2026</u></p> <p>The Business Services Teams are a high performing team and in a number of areas clear queues on a daily basis and for the majority of other areas, requests are actioned well within a 5 day turnaround time. Feedback from customers/colleagues is positive. For these reasons KPI's have not previously been introduced. Following on from this recommendation, KPI's for each Business Services Team are currently being finalised and will be ratified by CTU SLT before publication/ implementation. Once approved, they will be implemented to measure performance within the teams and reported on a monthly basis. If the KPI is not achieved, commentary will be added to explain why it has not been achieved.</p>
31	March 26	CTU Business Services	<p>A schedule of checks on user access permissions for systems and shared drives used by Business Services personnel will be established and undertaken at the defined intervals with records maintained to support the checks along with details of any corrective action taken.</p>	<p><i>Deputy Head of Business Services</i></p> <p>1/2/26</p>	<p><u>Update May 2026</u></p> <p>Shared Drive access permissions have been restricted to Business Services staff dependant on team and grade. Joiners and leavers are added/removed accordingly by IT on request.</p>

Ref	Original Report to JAC	Audit	Recommendation	Target Date /Responsible Officer	Latest position based on responses provided by management
					<p>Access permissions to add or remove individuals on MyTime &amp; Oracle are requested as &amp; when required with WMP IT. Audit reports are obtained by request from WMP to audit permissions on a more regular basis. Access permissions are removed for leavers from CTU or department (If moved roles internally to CTU).</p> <p><i>Internal Audit awaiting evidence to close action</i></p>