Agenda Item 5

Office of the Police, Fire & Crime Commissioner for Northamptonshire, Northamptonshire Commissioner Fire & Rescue Authority and Northamptonshire Police

Internal Audit Progress Report

Joint Independent Audit Committee – 01 July 2026

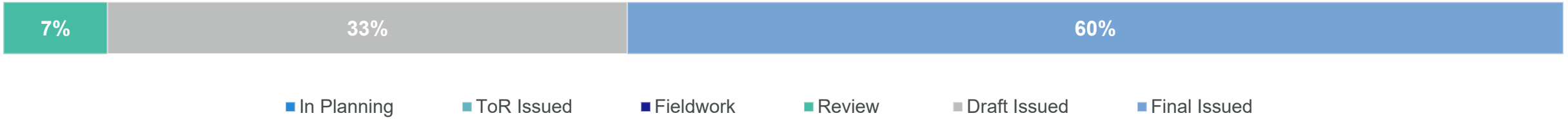
Date Prepared: June 2026

forvis mazars

Contents

01. Snapshot of Internal Audit Activity 2025/26

Below is a snapshot of the current position of the delivery of the 2025/26 Internal Audit Plan (Plan).



JIAC actions needed

- Note the progress being reported and consider final reports included separately in the Appendix 1.

RAG status of delivery of plan to timetable — **On Track**

Key Updates

Since the last update provided to the committee, we have issued the final report for the FOI/SAR, Digital Forensics, Joint Core Financials and NCFRA Prevention audits. Draft Reports have been issued for the IT Legacy Systems, Misconduct Hearings, Joint IT Cyber Governance, NCFRA Disciplinary Process & Management and Project Management audits. The NCFRA Workforce Plan audit is in review.

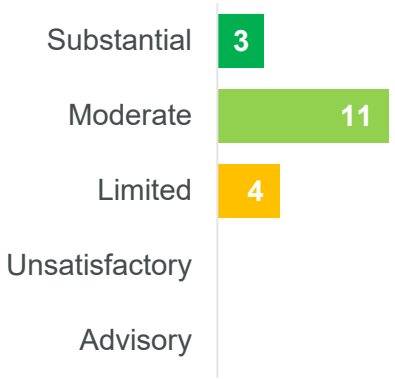
We have separately provided our Annual Conclusion within the **Annual Report,** and this paper also includes an overview of the Internal Audit Plan.

Collaboration Plan

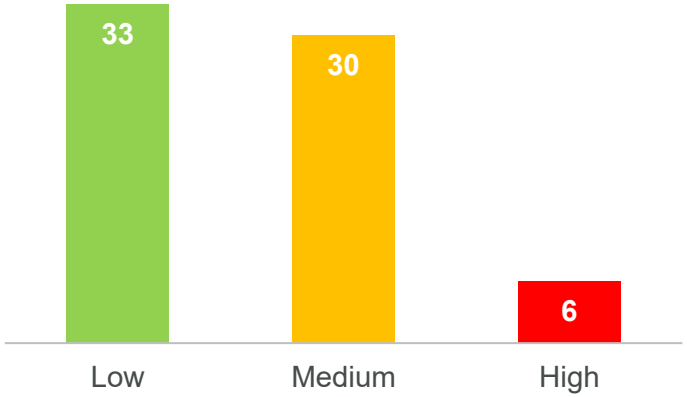
Since the last update provided to the committee, we have issued the final reports for the ESMOU POCA Income and EMSOU Forensics Accreditation audits.

An overview of the Collaboration Audit Plan can be found in **Section 3**.

Assurance opinions to date



Recommendations to date



02. Latest Reports Issued – Summary of Findings

FOI / SAR 2025/26

Your One Page Summary

Audit Objective: To assess the design and effectiveness of the control framework for FOI and SAR case management.

Audit rationale

Why the Audit is in Your 2025/26 Plan

Following multiple issues regarding disclosure of information through FOI and SAR legislation, resulting in corporate offence of contempt of court found against Chief Constable.

Summary of our opinion

Limited Opinion

See Appendix A1 for definitions

Summary of Recommendations

High (Priority 1)	1
Medium (Priority 2)	3
Low (Priority 3)	3

Actions agreed by you	100%
High Priority completion	July 2026
Overall completion	October 2026

Summary of findings

Examples of good practice

- ✓ ADISCO management tool in place to monitor and log Freedom of Information and Subject Access Requests. Full audit trail of each request is available.
- ✓ Egress tool for transmission of large data files.
- ✓ Audit plan in place for matters relating to information and data security.

Highest Priority Findings

- From a sample of 15 FOIs and 15 SARs we noted four instances of non-timely responses.
- From a sample of 15 SARs and 5 SAR internal review we noted three occasions of redaction errors in parts of the response.
- A review of 15 FOIs found that three were not published or disclosed publicly after the response.

Key root causes

- Resourcing and capacity issues within the Information Management Unit
- Redaction is a manual process

02. Latest Reports Issued – Summary of Findings

Digital Forensics 2025/26

Your One Page Summary

Audit Objective: To assess the design and effectiveness of the control framework for the Digital Forensics Unit (DFU).

Audit rationale

Why the Audit is in Your 2025/26 Plan	Your Strategic Risk	Your Strategic Objective
Following a period of significant backlogs in cases and issues with the storage and transport of digital evidence, the audit reviewed the controls in place for receiving, recording, processing and storing digital evidence.	CRR0037 - Digital Forensics Unit CRR0070 - DFU Data Storage and Transfer	Effective and Efficient Response

Summary of our opinion

Moderate Opinion
See Appendix A1 for definitions

Summary of Recommendations

High (Priority 1)	-
Medium (Priority 2)	3
Low (Priority 3)	2

Actions agreed by you	100%
High Priority completion	N/A
Overall completion	March 2027

Summary of findings

Examples of good practice

- ✓ The Detective Inspector holds weekly performance meetings with the DCI.
- ✓ Requests for Digital Media Investigators (DMIs) are formally routed through LANDesk or the Team inbox.
- ✓ A THINK DMI guidance sheet is published on the intranet and embedded in DMI email signatures, increasing consistency in when and how DMIs are deployed.
- ✓ Extracted data is stored on master and working hard drives, physically separated into different secure locations requiring swipe-card access.

Highest Priority Findings

- The Digital Forensic Policy and Digital Forensic Procedure require updates.
- Training compliance rates are not tracked.
- Exhibit locations on Niche and LANDesk do not align.

Key root causes (please refer to Section 02)

- The Statutory Code of Practice was updated in October 2025, after the updates to the Policy and Procedure in July 2025
- The Force does not have a list of roles that must be PIP1/PIP2 trained, so compliance cannot be calculated.
- Historic training records that pre-date 2018/2021 are not maintained.
- Oversight by the Digital Hub staff who did not check out the exhibit to the OIC.
- Oversight by Digital Hub staff member who has not filled in the laminated card.

02. Latest Reports Issued – Summary of Findings

Joint Core Financials 2025/26

Your One Page Summary

Audit Objective: To assess the design and effectiveness of the control framework for Joint Financial Controls specifically testing general ledger, payments, and payroll.

Audit rationale

Why the Audit is in Your 2025/26 Plan	Your Strategic Risk	Your Strategic / Tactical Objective
To assess the adequacy and effectiveness of the systems of internal control in operation to manage the core financial systems.	CRR0013 - Medium Term Financial Plan OP1005 - Long term sustainability of Northamptonshire Police funding	NCFRA - Making the Best of our Resources OPFCC – Modern Services that are Fit for the Future

Summary of our opinion

Moderate Opinion
See Appendix A1 for definitions

	X	

Summary of Recommendations

High (Priority 1)	-
Medium (Priority 2)	3
Low (Priority 3)	3

Actions agreed by you	100%
High Priority completion	N/A
Overall completion	December 2026

Summary of findings

Examples of good practice

- ✓ From a sample of 10 starters for both Police and Fire we noted they were appropriately paid.
- ✓ From a sample of 10 general ledger entries for both Police and Fire we noted appropriate backup evidence.
- ✓ From a sample of 10 new suppliers for both Police and Fire authorisation in accordance with procedures was available.

Highest Priority Findings

- Expense claims being made without sufficient evidence or receipts
- Lack of approval required for police overtime claims

Key root causes

- Self-approval of expense claims/overtime claims

Direction of travel

Previous Audit	Direction of Travel	Recurring Findings
November 2024	⇔ Previous Opinion: Moderate	• N/A

02. Latest Reports Issued – Summary of Findings

NCFRA Prevention 2025/26

Your One Page Summary

Audit Objective: To review the design and effectiveness of the control framework in relation to Prevention activities under home fire safety visits (HFSVs).

Audit rationale

Why the Audit is in Your 2025/26 Plan	Your Strategic Risk	Your Strategic / Tactical Objective
Following actions taken by the Service in response to adverse findings by HMICFRS inspection for 2023-25, specifically the "Requires Improvement" grading for "Preventing Fires and Other Risks".	SR26 - Failure to adequately safeguard children and "adults at risk"	We will help people stay safe from fire and other emergencies.

Summary of our opinion

Moderate Opinion

See Appendix A3 for definitions

Summary of Recommendations

High (Priority 1)	-
Medium (Priority 2)	2
Low (Priority 3)	2

Actions agreed by you	100%
High Priority completion	N/A
Overall completion	October 2027

Summary of findings

Examples of good practice

- ✓ A Home Fire Safety Visits (HFSV) Policy (June 2025) is in place.
- ✓ NCFRA has HFSV Guidance Notes (April 2025) in place which provides direction for a number of relevant operational activities, including carrying out HFSVs and recording HFSVs.
- ✓ Ownership of HFSVs is considered to be within Community Risk Groups.

Highest Priority Findings

- Lack of assurance over accuracy of HFSV eLearning training records.
- Data integrity issues with HFSV data.

Key root causes

- Absence of system integration between Moodle and RedKite.[1]
- Lack of formal controls to validate training completion and recording.
- System configuration gaps.
- Lack of period data integrity checks.

[1] Moodle is used to access HFSV related eLearning training and RedKite is used to record training completion.

02. Latest Reports Issued – Summary of Findings

EMSOU POCA Income 2025/26

Your One Page Summary

Audit Objective: To assess the design and effectiveness of the control framework for POCA income in place at the East Midlands Special Operations Unit (EMSOU).

Audit rationale

Why the Audit is in Your 2025/26 Plan

Concerns regarding the receipting, recording and managing income received under the Proceeds of Crime Act 2002 (POCA); particularly related to income received through the Asset Recovery Incentivisation Scheme (ARIS).

Summary of our opinion

Moderate Opinion

See Appendix A1 for definitions

Summary of Recommendations

High Priority	-
Medium Priority	1
Low Priority	2

Actions agreed by you	100%
High Priority completion	N/A
Overall completion	July 2026

Summary of findings

Examples of good practice

- ✓ ARIS income is reported to the East Midlands Police Collaboration PCC and CC Board meetings.
- ✓ From a sample of six cash seizures, we noted that deposit forms were in place from the investigating officer.
- ✓ Reconciliations are conducted every month on the EMSOU current and deposit account.
- ✓ We reconciled Q3 and Q4 ARIS income for 2024/25 to the Home Office remittance.

Highest Priority Findings

- Lack of records provided or communication with auction house once asset is sold.
- Lack of record of sold assets.
- Reconciliation procedure not reviewed.

Key root causes

- Lack of record keeping and communication channels, especially in the case of a joint investigation

02. Latest Reports Issued – Summary of Findings

EMSOU Forensics Accreditation 2025/26

Your One Page Summary

Audit Objective: To assess the design and effectiveness of the control framework for forensic accreditation management at the East Midlands Special Operations Unit – Forensic Services (EMSOU-FS).

Audit rationale

Why the Audit is in Your 2025/26 Plan

This review will provide assurance regarding the Unit's control framework in place for managing, achieving and maintaining forensic accreditation.

Summary of our opinion

Substantial Opinion
See Appendix A1 for definitions

X

Summary of Recommendations

High (Priority 1)	-
Medium (Priority 2)	-
Low (Priority 3)	1

Actions agreed by you	100%
High Priority completion	N/A
Overall completion	March 2027

Summary of findings

Examples of good practice

- ✓ Training, competency and quality assurance procedures are in place for each forensic area.
- ✓ A range of governance structures are in place to oversee forensic accreditation, including the quarterly Regional SAI Accreditation Group, biannual Management Review Meetings, monthly Quality Meetings, and monthly EMSOU-FS Accreditation Meetings.
- ✓ Budget for forensic accreditation is allocated as part of the Unit's annual budget setting process, with specific budgets for each forensic area. We confirmed this is monitored as part of monthly Budget Monitoring Reports for individual forces.
- ✓ The Quality Team complete internal audits on accredited areas on a four-year cycle. This includes review of quality and technical processes and procedures to ensure compliance with accredited standards.
- ✓ Non-conforming actions arising from internal audits and annual UKAS visits are logged on quality management system, BizzMine.
- ✓ EMSOU-FS has already achieved accreditation in ISO17020 across 4/10 bases and are working with UKAS to expand this over the coming years, as well as including all the aspects of the INC-100 minimum scope to achieve compliance by April 2027.

Low Priority Finding

- No accreditation strategy or implementation plan in place outlining how the Unit will work towards achieving and maintaining accreditation compliance.

Key root causes

- The Unit's strategic approach to forensic accreditation has not been formally defined.

03. Overview of Collaboration Plan 2025/26

The table below lists the status of all reviews within the 2025/26 Collaboration Plan.

Review	Original Days	Revised Days	Status	Original Quarter	Start Date	JIAC	Assurance Level	Total	High	Medium	Low
EMSOU POCA Income	10	10	Final	Q2	18-Sep-25	Jul-26	Substantial	1	-	-	1
EMSOU Forensics Accreditation	10	10	Final	Q3	09-Mar-26	Jul-26	Moderate	3	-	1	2
Totals	**20**	**20**					**Totals**	**4**	**-**	**1**	**3**

04. Key Performance Indicators 2025/26

We monitor key areas of performance and delivery in line with the KPIs/Service Levels set out in our contract with the Office of the Police, Fire & Crime Commissioner for Northamptonshire, Northamptonshire Commissioner Fire & Rescue Authority and Northamptonshire Police. Latest summary figures have been set out below:

KPI	KPI/SLA description	Criteria	Performance
1	Annual report provided to the JIAC	As agreed with the Client Officer	July 2025
2	Annual Operational and Strategic Plans to the JIAC	As agreed with the Client Officer	March 2025
3	Progress report to the JIAC	7 working days prior to meeting	Achieved
4	Issue of draft report	Within 10 working days of completion of exit meeting	86% (12 / 14)
5	Issue of final report	Within 5 working days of agreement of responses	89% (8 / 9)
6	Audit Brief to auditee	At least 10 working days prior to commencement of fieldwork	60% (9 / 15)
7	Customer satisfaction (measured by survey) “Overall evaluation of the delivery, quality and usefulness of the audit” Very Good, Good, Satisfactory, Poor or Very Poor	85% average with Satisfactory response or above	100% (1 / 1)

04. Key Performance Indicators 2025/26 (Cont.)

Review	Date of ToR	Start of Fieldwork	Days Notice (10)	Exit Meeting	Draft Report	Time from Close to Draft Report (10)	Management Comments Received	Time to Received Comments (15)	Final Report Issued	Time Taken to Issue Final Report (5)
Office of the Police, Fire and Crime Commissioner for Northamptonshire and Northamptonshire Police										
Accreditation Management	16-May-25	27-May-25	6	01-Aug-25	11-Sep-25	18	20-Nov-25	50	21-Nov-25	0
Seized Property	17-Jul-25	26-Aug-25	27	09-Sep-25	30-Sep-25	9	16-Oct-25	12	24-Oct-25	3
IT - Legacy Systems	21-Oct-25	24-Nov-25	24	24-Mar-26	01-Apr-26	4				
Control Room / First Contact	21-Nov-25	08-Dec-25	11	29-Jan-26	30-Jan-26	0	17-Feb-26	12	17-Feb-26	0
FOI / SAR	17-Dec-25	12-Jan-26	15	10-Feb-26	25-Feb-26	7	11-Mar-26	10	13-Mar-26	1
Digital Forensics	12-Jan-26	22-Jan-26	8	16-Mar-26	31-Mar-26	7	01-Mar-26	21	7-May-26	3
Misconduct Hearings	19-Mar-26	08-Apr-26	12	20-May-26	28-May-26	4				
Joint Audits										
Fleet Management	16-May-25	02-Jun-25	10	08-Sep-25	30-Sep-25	10	23-Oct-25	17	30-Oct-25	3
Core Financials	30-Oct-25	10-Nov-25	18	02-Jan-26	16-Jan-26	6	21-Apr-26	65	23-Apr-26	2
IT - Cyber Governance	21-Oct-25	12-Jan-26	56	06-Apr-26	09-Jun-26	28				

04. Key Performance Indicators 2025/26 (Cont.)

Review	Date of ToR	Start of Fieldwork	Days Notice (10)	Exit Meeting	Draft Report	Time from Close to Draft Report (10)	Management Comments Received	Time to Received Comments (15)	Final Report Issued	Time Taken to Issue Final Report (5)
Northamptonshire Commissioner Fire & Rescue Authority										
Data Quality & Management Information	17-Jul-25	29-Jul-25	8	27-Oct-25	30-Oct-25	3	12-Nov-25	9	21-Nov-25	4
Prevention	04-Nov-25	10-Nov-25	4	18-Dec-25	14-Jan-26	6	05-Mar-26	36	15-Apr-26	17
Workforce Plan	13-Jan-26	26-Jan-26	9							
Disciplinary Process & Management	13-Mar-26	07-Apr-26	15	27-Apr-26	15-May-26	9				
Project Management	08-Apr-26	20-Apr-26	8	15-May-26	28-May-26	6				

05. Snapshot of Internal Audit Activity

Below is a snapshot of the current position of the delivery of the 2026/27 Internal Audit Plan (Plan).

JIAC actions needed

- Note the progress being reported and consider final reports included separately in the Appendix 1.

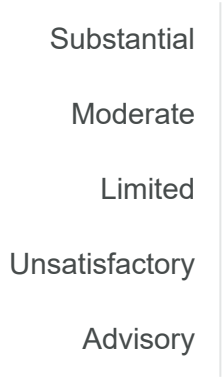
RAG status of delivery of plan to timetable — **On Track**

Key Updates

Since presenting the plan to the committee, fieldwork is underway for the Investigations audit and VAWG Strategy audits. We continue to plan and scope the remaining audits from the 2026/27 plan. An overview of the Internal Audit Plan can be found in **Section 6**.

We have presented our collaboration plan for 2026/27 to the Regional CFOs and FDs at their meeting on 26 February 2026, we continue to plan and scope the audits from the 2026/27 plan. An overview of the Collaboration Audit Plan can be found in **Section 7**.

Assurance opinions to date



Recommendations to date

06. Overview of Internal Audit Plan 2026/27

The table below lists the status of all reviews within the 2026/27 Plan.

Review	Original Days	Revised Days	Status	Original Quarter	Start Date	JIAC	Assurance Level	Total	High	Medium	Low
Office of the Police, Fire & Crime Commissioner for Northamptonshire and Northamptonshire Police											
Investigations	10	10	Fieldwork	Q1	26/05/2026						
VAWG Strategy	10	10	Fieldwork	Q1	15/06/2026						
IT - Access Control	10	10	In Planning	Q1	TBC						
Health & Safety	10	10	In Planning	Q2	13/08/2026						
PSD Complaints	10	10	In Planning	Q3	05/10/2026						
Data Management	10	10	In Planning	Q3	06/11/2026						
Reasonable Adjustments	10	10	In Planning	Q4	12/01/2027						
Sustainability	10	10	In Planning	Q4	13/01/2027						
Firearms Licensing	10	10	In Planning	Q4	02/02/2027						
Accreditation Management Follow Up	7	7	In Planning	Q4	TBC						
IT - Follow Up	7	7	In Planning	Q4	TBC						
Totals	**104**	**104**					**Totals**	**-**	**-**	**-**	**-**

06. Overview of Internal Audit Plan 2026/27 (Cont.)

The table below lists the status of all reviews within the 2026/27 Plan.

Review	Original Days	Revised Days	Status	Original Quarter	Start Date	JIAC	Assurance Level	Total	High	Medium	Low
Joint Audits											
Core Financials	20	20	In Planning	Q2	24/08/2026						
Occupational Health & Wellbeing	20	20	In Planning	Q3	12/10/2026						
IT - Disaster Recovery	20	20	In Planning	Q3	TBC						
Northamptonshire Commissioner Fire & Rescue Authority											
Budget Setting / MTFP	10	10	In Planning	Q1	23/09/2026						
Culture & Governance	10	10	In Planning	Q2	21/09/2026						
Specialist Training & CPD	10	10	In Planning	Q4	17/02/2027						
JESIP and Major Incidents	15	15	In Planning	Q4	22/02/2027						
Totals	**105**	**105**					**Totals**	**-**	**-**	**-**	**-**

07. Overview of Collaboration Plan 2026/27

The table below lists the status of all reviews within the 2026/27 Collaboration Plan.

Review	Original Days	Revised Days	Status	Original Quarter	Start Date	JIAC	Assurance Level	Total	High	Medium	Low
EMSOU Digital Forensics	10	10	In Planning	Q2	10-Aug-26						
East Midlands Police Legal Services (EMPLS)	10	10	In Planning	Q3	16-Nov-26						
Totals	**20**	**20**					**Totals**	**-**	**-**	**-**	**-**

08. Key Performance Indicators 2026/27

We monitor key areas of performance and delivery in line with the KPIs/Service Levels set out in our contract with the Office of the Police, Fire & Crime Commissioner for Northamptonshire, Northamptonshire Commissioner Fire & Rescue Authority and Northamptonshire Police. Latest summary figures have been set out below:

KPI	KPI/SLA description	Criteria	Previous Score
1	Annual report provided to the JIAC	As agreed with the Client Officer	July 2026
2	Annual Operational and Strategic Plans to the JIAC	As agreed with the Client Officer	March 2026
3	Progress report to the JIAC	7 working days prior to meeting	Achieved
4	Issue of draft report	Within 10 working days of completion of exit meeting	-
5	Issue of final report	Within 5 working days of agreement of responses	-
6	Audit Brief to auditee	At least 10 working days prior to commencement of fieldwork	50% (1 / 2)
7	Customer satisfaction (measured by survey) “Overall evaluation of the delivery, quality and usefulness of the audit” Very Good, Good, Satisfactory, Poor or Very Poor	85% average with Satisfactory response or above	-

08. Key Performance Indicators 2026/27 (Cont.)

Review	Date of ToR	Start of Fieldwork	Days Notice (10)	Exit Meeting	Draft Report	Time from Close to Draft Report (10)	Management Comments Received	Time to Received Comments (15)	Final Report Issued	Time Taken to Issue Final Report (5)
Office of the Police, Fire and Crime Commissioner for Northamptonshire and Northamptonshire Police										
Investigations	21/05/2026	26/05/2026	2							
VAWG Strategy	01/06/2026	15/06/2026	10							
IT - Access Control		TBC								
Health & Safety		13/08/2026								
PSD Complaints		05/10/2026								
Data Management		06/11/2026								
Reasonable Adjustments		12/01/2027								
Sustainability		13/01/2027								
Firearms Licensing		02/02/2027								
Accreditation Management Follow Up		TBC								
IT - Follow Up		TBC								

08. Key Performance Indicators 2026/27 (Cont.)

Review	Date of ToR	Start of Fieldwork	Days Notice (10)	Exit Meeting	Draft Report	Time from Close to Draft Report (10)	Management Comments Received	Time to Received Comments (15)	Final Report Issued	Time Taken to Issue Final Report (5)
Joint Audits										
Core Financials		24/08/2026								
Occupational Health & Wellbeing		12/10/2026								
IT - Disaster Recovery		TBC								
Northamptonshire Commissioner Fire & Rescue Authority										
Budget Setting / MTFP		23/09/2026								
Culture & Governance		21/09/2026								
Specialist Training & CPD		17/02/2027								
JESIP and Major Incidents		22/02/2027								

09. Definitions of Assurance Levels and Recommendation Priority Levels

Definitions of Assurance Levels	
Substantial Assurance	The framework of governance, risk management and control is adequate and effective.
Moderate Assurance	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Limited Assurance	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.
Unsatisfactory Assurance	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

Definitions of Recommendations		
High (Priority 1)	Significant weakness in governance, risk management and control that if unresolved exposes the organisation to an unacceptable level of residual risk.	Remedial action must be taken urgently and within an agreed timescale.
Medium (Priority 2)	Recommendations represent significant control weaknesses which expose the organisation to a moderate degree of unnecessary risk.	Remedial action should be taken at the earliest opportunity and within an agreed timescale.
Low (Priority 3)	Recommendations show areas where we have highlighted opportunities to implement a good or better practice, to improve efficiency or further reduce exposure to risk.	Remedial action should be prioritised and undertaken within an agreed timescale.

A1

Latest Reports Issued – Detailed Findings

FOI / SAR 2025/26

Ref	Recommendation	Priority	Management Comments	Due Date
1	The ICO recommends that Subject Access Requests are responded to within one calendar month. For complex cases this can be extended by notifying the requestor. Similarly, the Force Freedom of Information Policy (November 2025) states that requests should be responded to usually within 20 working days. We selected a sample of 15 subject access requests from June 2025 and December 2025 and noted that three were responded to more than a calendar month later. We also selected a sample of 15 freedom of information requests from June 2025 and December 2025 and noted that four were responded to more than 20 working days later. We noted in one case (21870) that a FOI received in November 2025 had still not been closed – leading the requestor to appeal. Furthermore, we analysed a report of all closed FOIs and SARs from ADISCO from June 2025 to December 2025. We found: • From 868 closed FOIs, 419 had been responded to after the due date. • From 738 closed SARs, 286 had been responded to after the due date. We were advised by the Head of Information Assurance that there has been a significant backlog of requests, and that the department has been short staffed. Audit noted that ADISCO has a monthly stats viewer which shows the number of FOIs or SARs which have been closed out of time. We noted that these figures have just begun to be reported to the Information Assurance Board, as of January 2026. **The Force should:** **1. Report timeliness of FOIs and SARs to the Information Assurance Board** **2. Formulate and communicate a recovery plan to deal with overdue requests**	**High**	Management acknowledges the audit findings relating to timeliness and backlog management and accepts that performance during the review period did not consistently meet statutory expectations. A recovery position has already been initiated, including: • Introduction of regular performance reporting using ADISCO data. • Escalation of FOI and SAR performance through established information governance forums and Gold Group • Active management focus on backlog reduction and prioritisation of aged cases. <u>Actions:</u> 1. We will develop, implement, and monitor a formal recovery and stabilisation plan, including structural solutions to address demand, capacity, and complexity 2. We will review progress regularly through established governance arrangements. *Trina Kightley-Jones – Head of Information Assurance*	01 July 2026
2	Third-party personal data should be redacted when disclosing a SAR, this can include, where applicable, names of individuals. From our sample of 15 SARs and five SAR appeals, we identified three instances where names that should have been redacted remained visible on specific pages or sections:	**Medium**	Management accepts the audit findings regarding manual redaction processes and acknowledges the inherent risk of human error in this area. Current controls rely heavily on individual expertise and manual checking, which is not optimal given the increasing volume and complexity of digital material, including BWV.	01 September 2026

FOI / SAR 2025/26 (Cont.)

Ref	Recommendation	Priority	Management Comments	Due Date
	• 25/16967: Officer name not redacted. • 25/12239: Third-party name not redacted. • 25/16371: Third-party name within a witness statement was not redacted. The team advised that this was down to human error. We were further advised by management that the Force is considering the use of external tools which would help officers manage redactions. **The Force should:** **1. Implement redaction training to staff involved in responding to SARs.** **2. Consider the use of external tools to support with the redaction process.**		Actions: Management agrees that additional mitigations are required and will: 1. Strengthen targeted redaction training for staff involved in SAR responses. 2. Explore and assess technical solutions to support and automate elements of the redaction process, subject to assurance, cost and value for money considerations. In the interim, quality assurance expectations will be reinforced to reduce the likelihood of repeat errors. *Trina Kightley-Jones – Head of Information Assurance*	
3	The FOI policy (November 2025) states that if there is wider public interest in topics based on reports/media or to provide useful context then the response can be sent to the Corporate Communications team for them to identify public interest. The Force will publish FOI response via the public facing website to make information available proactively. From our sample of 15 FOI requests completed between June 2025 and January 2026, we identified multiple instances where no public disclosure was made and no adequate rationale was recorded for withholding publication. These included: • 25/18418: FOI regarding bulk fuel purchases (response issued October 2025) • 25/16953: FOI regarding Palestine Action costs and arrests (response issued September 2025) • 25/14724: FOI regarding honour-based abuse (response issued August 2025) **The Force should ensure that FOIs, where applicable and for the public interest, are published online. Where there is no wider public interest, this should be clearly documented within ADICSO**	**Medium**	Management accepts the finding that public disclosure of FOIs has not been consistently applied, particularly during periods of backlog pressure. This has been driven primarily by prioritisation of statutory response deadlines over publication activity. Management agrees that this approach is not sustainable and can create additional demand through repeat requests. Action: We will identify FOIs suitable for public disclosure, ensure that the rationale is documented when publication is not appropriate, and integrate publication activities into routine FOI processes *Trina Kightley-Jones – Head of Information Assurance*	01 July 2026
4	Section 11 of the Data Protection Policy (2022) states that to comply with legislative and policy requirements there shall be regular audit regime within the force, led by auditors.	**Medium**	Management accepts that, while information security audits are undertaken, formal reporting and tracking of audit findings and actions has not yet fully matured.	01 July 2026

FOI / SAR 2025/26 (Cont.)

Ref	Recommendation	Priority	Management Comments	Due Date
	We noted that audits are conducted by the Information Security team. We reviewed the 2025 audit plan and were advised by management that this was risk based. We selected a sample of two audits, from the five which were completed, site Security Access and PAVA, to review whether there were reports and recommendations. We noted that currently there is no formal mechanism to report findings and monitor recommendation implementation status, to senior management. **The Force should ensure that audits relating to information security are monitored and regularly reported to the Information Assurance Board.**		This reflects the recent implementation of new audit approaches rather than an absence of intent. Management agrees that improvements are required to ensure: • Clear visibility of audit outcomes. • Active monitoring of recommendation implementation. • Appropriate escalation through governance forums. Action: We will formalise and implement audit reporting and oversight arrangements ensuring all information security audits are documented, regularly monitored, and reported at each quarterly Information Assurance Board meeting, in order to strengthen assurance and support organisational learning. *Trina Kightley-Jones – Head of Information Assurance*	

We have also raised three Low priority recommendations regarding:

- The Force should ensure that fields such as received date, and due date, within ADISCO are made mandatory to ensure that they are completed, and allow for SARs to be better monitored.
- The Force should ensure that the Data Protection Policy and Subject Access Request Policy are regularly reviewed by the Head of Information Assurance and are consistent with changes in ICO guidelines.
- The Force should develop a plan which establishes consistent training requirements for new starters within the Information Management Unit.

Digital Forensics 2025/26

Ref	Recommendation	Priority	Management Comments	Due Date
1	Up-to-date Policies and Procedures are important to ensuring that all forensic work is completed lawfully and consistently. For the Digital Forensics Unit (DFU), this includes aligning documentation with the requirements of the Forensic Science Regulator Act (FSR) 2021 and the associated Statutory Code of Practice. We reviewed the Digital Forensic Policy and Digital Forensic Procedure and note the following: <u>Digital Forensic Policy & Procedure:</u> The Policy and Procedure documents state that it was last reviewed in July 2025; however, the Force Directory records indicate that the Policy was last updated in January 2026 and the Procedure in September 2025. We were advised by the Detective Inspector (DI) that this discrepancy is due to an update made by the Library Team. The DI has since updated the review date so that the document will be reviewed annually in July 2026, in line with Force best practice. <u>Digital Forensics Policy:</u> The Policy does not reference the Forensic Science Regulator Act 2021 or the Statutory Code of Practice, which are legal requirements from October 2025. The DI advised that the Policy requires a full refresh and update as Section C2 of the Code is in place. <u>Digital Forensic Procedure:</u> The Procedure mentions FSR 2021 and its Code of Practice but does not define mandatory compliance, method validation, verification and non-conformance handling. The DI advised that the Procedure will be updated for the July 2026 refresh. We noted that the Procedure document refers to itself as “this policy” throughout. The DI advised that this terminology will be corrected as part of the July 2026 updates.	**Medium**	The policy and Procedure needs to be updated with reference to both the FSR and Codes. This will be completed prior to the review of both. *DI Tom Curlett-New – Head of Digital Hub*	01 July 2026

Digital Forensics 2025/26 (Cont.)

Ref	Recommendation	Priority	Management Comments	Due Date
	The Digital Forensic Policy and Digital Forensic Procedure should be fully reviewed and updated to incorporate the requirements of the Forensic Science Regulator Act 2021 and the Statutory Code of Practice, ensuring that terminology, compliance expectations, validation processes, and quality management provisions are reflected.			
2	It is important for the Force to deliver training to frontline officers on the appropriate identification and seizure of digital devices and evidence, so that they can correctly recognise sources of digital data and handle them to preserve evidential integrity. The Learning and Development (L&D) are responsible for delivering training inputs to new frontline officers. We were provided with training data, and note the following: • Number of frontline officers PIP1 trained: A total of 1,075 frontline officers have completed PIP1 training, with 1,074 of these trained from 2013 onwards. The L&D team could only locate training materials dating back to July 2018, there are 680 officers trained since July 2018. • Number of frontline officers PIP2 trained: A total of 366 frontline officers have completed PIP2 training; however, this figure includes PIP2-qualified officers across all ranks. At the constable and sergeant levels, 297 officers are recorded as trained. The L&D team advised that training timetables only date back to December 2021. Although they believe PIP2 training was delivered prior to this date, no supporting evidence could be located. Based on available records, 139 officers have completed PIP2 training since December 2021. • Frontline officers that are not trained in either: There are 163 frontline officers who are not recorded as having completed either PIP1 or PIP2 training. Management advised that, it is likely these officers either received training delivered prior to PIP1 being formally implemented or have transferred into Northamptonshire Police without their training records being updated in the L&D system.	**Medium**	Up to date list is to be compiled, as well as process for PIP1/PIP2 officer training. Reporting to senior management to be in place as well. *Inspector Damian Hiscocks – L&D*	31 July 2026

Digital Forensics 2025/26 (Cont.)

Ref	Recommendation	Priority	Management Comments	Due Date
	For each of the categories above, we sought to establish the full population of staff who are expected to be trained in order to calculate a compliance percentage. The DI and L&D team advised they do not know the total number of officers required to be trained, meaning compliance rates for PIP1, PIP2, and untrained officers are not tracked. **The Force should:** **1. Establish an up-to-date list of all frontline officers who are required to receive PIP1 and PIP2 training.** **2. Develop a process to record, monitor and report training completion and compliance rates for PIP1 and PIP2** **3. Introduce regular reporting to senior management to offer assurance that frontline officers maintain the required competencies for identifying and seizing digital evidence.**			
3	It is important that the movement and location of exhibits are tracked by updating LANDesk, as this ensures continuity of evidence throughout the forensic process. We reviewed the NOR-TP-77 Exhibit Handling Procedure (December 2024). It outlines the requirements for the storage of exhibits, stating that once Digital Hub staff have completed receipting and processing, exhibits must be placed in a secure exhibit store. Items should be stored on the shelving units. Once an item is placed on the shelf, staff are required to update the LANDesk location and record the LANDesk case reference number on the laminated shelf card. We selected a sample of ten exhibits held at the DFU on Niche. We noted that nine exhibits were stored in the correct physical location, as recorded on LANDesk. However, for one exhibit (95724), we found that it had been returned to the Officer in Charge (OIC). While this change had been updated on LANDesk, it had not been updated on Niche, which continued to show the exhibit as being held at the DFU.	**Medium**	Jo will include an entry into NOR-TP-77 but also NOR-WI-06 which is the more detailed working instruction for returning exhibits. Jo has already completed the second part and will share the evidence. *Jo Hanson – Digital Hub Compliance Manager*	01 July 2026

Digital Forensics 2025/26 (Cont.)

Ref	Recommendation	Priority	Management Comments	Due Date
	. We were advised by the Compliance Manager that Digital Hub staff can check exhibits out to the officer collecting the item. However, this procedural guidance is not included in the NOR-WI Exhibit Returns Procedure. Rather, the procedure states that LANDesk should be updated when an exhibit is returned to the OIC but does not clarify who is responsible for updating LANDesk. We also identified one instance (92464) where the laminated card on the shelf had not been filled out, the Compliance Manager advised that this was an oversight by the Digital Hub staff member. **The Force should:** **1. Update NOR-TP-77 Exhibit Handling Procedure to include the Digital Hub staff responsibility for checking out exhibits to an OIC once collected and share the updated procedure to staff.** **2. Remind Digital Hub staff to record the LANDesk case reference number on the laminated shelf card.**			

We have also raised two Low priority recommendations regarding:

- The Force should:
    1. Introduce role-based access controls within the Digital Forensics Unit to ensure that staff only have access to the specific rooms and storage areas required for their duties.
    2. Explore options to upgrade or reconfigure the current access control system, ensuring it can support more granular access groups.
- The Force should ensure that LANDesk audits are completed on a six-monthly basis, and document evidence of completion.

Joint Core Financials 2025/26

Ref	Recommendation	Priority	Management Comments	Due Date
1	The Force Expenses and Allowances Policy (October 2025) states that only in exceptional circumstances will expenses be paid without a receipt, and in such cases the appropriate budget managers authorisation is required. The Service Pay and Allowances Policy (December 2024) also states that expenses will only be paid with a receipt. Expenses are made on a self-service portal, and no prior authorisation is required. We were advised that the Senior Accountant audits a sample of expense claims every month. We selected a sample of 21 expense claims from April 2025 to September 2025 made within the Force., We sought to confirm the claims were legitimate and had sufficient evidence as per the expenses policy 2025. We noted seven exceptions across our testing for this: • 34-5007729 April 2025: £110.79 claimed for various lunches without receipt • 34-5000247 April 2025: £237.67 claimed for National surveillance court without receipt • 34-5008523: April 2025: £19.69 claimed for evening meal without receipt • 34-5007653: May 2025: £43.55 claimed for breakfast without receipt • 34-5000721: August 2025: £1,008 for mileage but incorrect postcode provided • 34-5008631: August 2025: £147.84 claimed for 14 different subsistence but without receipt • 34-5008968: August 2025: £58.94 claimed for expenses but without receipt We also selected a sample of 10 fire expense claims from April 2025 to September 2025. Again, we noted two occasions where there is inadequate evidence of receipt or milage claim detail: • 23-1800172 April 2025: £107.55 claimed for mileage but there was a lack of detail as just stated ‘Home Fire Safety visits’ • 23-1809044 May 2025: £76.79 claimed for congestion charge without receipt	**Medium**	MHR, our payroll provider, have been approached regarding the limitations of the system, who have confirmed that receipt attachments cannot be made mandatory. We continue to investigate this to understand if there are any other controls that can be put in place within the self-serve system. As a result of this expenses will continue to be audited within the finance team to ensure no fraudulent claims are made. *Sam Ashby-Clarke – Head of Finance*	31 March 2026

Joint Core Financials 2025/26 (Cont.)

Ref	Recommendation	Priority	Management Comments	Due Date
	1. The Force and NCFRA should explore an option within the self-service portal that would make it mandatory for receipts to be uploaded. **2. The finance and payroll team should continue to audit claims, including mileage details of postcodes, and locations.**			
2	We conducted a walkthrough with a member of the enabling services team and noted that currently there is not an approval system for approving overtime. Police officers submit their claims within the overtime claim form. They would select the type of claim they are making and the rate for which this is applicable. The Overtime system does create an exception report if a member of staff has selected the incorrect rate for the overtime. Furthermore, every month the top 10 claimants are also analysed. However, we noted that the system has no controls in place for an officer making legitimate but potentially fraudulent overtime claims due to there not being an approval process in place. **The Force should implement a wider monthly sample check of overtime claims to ensure they have been legitimately made.**	**Medium**	We acknowledge and note the recommendations made regarding overtime. The Head of Finance will review with the Head of HR to discuss this further in order to widen the checks that can be made on overtime through payroll. The Payroll team will continue to monitor and flag all large payments that are made each month, however, it is unlikely that all checks will remain retrospective, as it would not be viable to add in manager checks across the entire force and the Value for Money against the risk would not be worth while, given that we have had very low levels of concerns flagged to PSD for any form of misconduct. *Sam Ashby-Clarke – Head of Finance*	30 June 2026
3	Manual and urgent payments require an urgent payment request form that would need to be completed by the requestor and sent to the finance team. We selected a sample of 10 police urgent payments from April to August 2025 to confirm they were appropriately requested and approved. We noted an exception in one case where a payment of £557 was made on the 26th of June 2025 to supplier without a request form. We were advised by management that this was an urgent request outside the Unit Four financial system as they were not set up as a supplier. Communications with the requestor noted that the supplier account had not been set up and therefore the invoices had not been added to the system, seemingly due to issues experienced by the requestor.	**Medium**	The finance team currently request that a payment request form is made before any one off payment is made, this is largely for payments that sit outside of the Accounts Payable ledger. In the instance noted the payment would have fallen under AP processes had the supplier been set up. It is important to note that for all manual/one off payment a spreadsheet is maintained which includes support for the payment (in this case the supporting evidence was the invoice). The payment is set up by one member of the finance team and approved by another member of the team, who review all the back up, which ensures segregation of duties.	31 March 2026

Joint Core Financials 2025/26 (Cont.)

Ref	Recommendation	Priority	Management Comments	Due Date
3	Payment was made with appropriate segregation of duties, following verification of payment details and of the services received, however it should be noted that payments shouldn't be made through urgent payments without a signed request form submitted to the finance team. **The Force should ensure that appropriate training is provided to staff members with access to Payables in Unit 4 so that supplier accounts can be created appropriately.**	**Medium**	Therefore the risk is not exacerbated by the missing form, however, the documentation, does provide better and more transparent processes and as such, where possible we will always use the standard forms. *Sam Ashby-Clarke – Head of Finance*	31 March 2026

We have also raised three Low priority recommendations regarding:

- The Force and NCFRA should ensure that the non-purchase order list is reviewed annually and updated if necessary.
- The Force and NCFRA should implement contingency measures in place when members of staff who are responsible for signing off reconciliations are away.
- The NCFRA should implement an automated workflow for fire supplier email changes to synchronise with police.

NCFRA Prevention 2025/26

Ref	Recommendation	Priority	Management Comments	Due Date
1	In its 2024 HMICFRS inspection, NCFRA received a finding that "station-based staff should have a better understanding of the prevention strategy," as operational staff advised the Inspectorate that they had "limited training or confidence" to complete HFSV activities. It is therefore important that a regular HFSV-specific training regime is in place and that systems enable accurate and valid recording of training access and completion, particularly for eLearning training. In March 2025, NCFRA rolled out person-centred HFSV eLearning training to be completed by firefighters, crew managers, watch managers, and relevant prevention staff every two years. Our data analytics of this training data found a compliance rate of approximately 92%. However, NCFRA currently uses two separate systems: Moodle (to access and complete the eLearning training) and RedKite (to record completion). As these systems are not integrated, there is a risk that individuals may record completion in RedKite without actually accessing and completing the training in Moodle. To assess this risk, we reviewed a sample of 14 individuals recorded as having completed the training and noted the following: • Four instances (three firefighters and one watch manager) where tracking data showed access times significantly below the minimum expected duration of 60 minutes (range: 18–41 minutes; average: 28.25 minutes). • Nine instances where the Moodle score was below 100%, despite staff having individually accessed and recorded training as complete. • Six instances where Moodle tracking data showed the eLearning status as incomplete, despite staff having individually accessed and recorded completion. • Five instances where Moodle records indicated the individual had never accessed the eLearning directly, yet RedKite recorded completion. Management advised this was likely due to group-based training delivered by watch managers at stations, which was supported by Moodle access records for the respective watch managers.	**Medium**	NFRS is aware of limitations in relation to the Moodle and Redkite platforms and these are informing the procurement process for a new LMS, this has commenced and is due to be in place by 1/10/2027. Dip sampling of training records will be facilitated in conjunction with the new Quality Assurance process for HFSVs which commenced in January 26. *Neil Sadler – Area Manager*	01 October 2027

NCFRA Prevention 2025/26 (Cont.)

Ref	Recommendation	Priority	Management Comments	Due Date
1 (ctd)	The Prevention, Safeguarding and Partnerships Manager advised that as budget approval has been obtained, NCFRA intends to begin procurement activities for a single learning management system, with market engagement beginning in early 2026. **NCFRA should:** **1. Explore options for an integrated Learning Management System (LMS) that includes system controls to ensure training can only be marked as complete once accessed in its entirety. This should be included as part of the LMS procurement process in 2026.** **2. Introduce periodic dip sampling for completed HFSV training data to validate accuracy and adherence.** **3. Investigate the four instances where tracking showed training was completed below the minimum expected duration of 60 minutes.** **4. Work with the suppliers of Moodle and RedKite to investigate the system issues around access and completion recording.** **5. Formalise and communicate procedures for recording group-based eLearning training to ensure consistency and transparency.**			
2	It is essential for organisations to maintain data that is complete, accurate, and formatted correctly, as this underpins reliable management reporting, supports informed decision-making, and enables identification of operational efficiencies. We reviewed the HFSV data (February 2025 – October 2025) and identified several data integrity issues (population 3439): • Blank mandatory fields which should be populated automatically. • Blank mandatory fields which should be populated manually. • Direct engagement jobs (116D) not completed automatically within 42 days as expected due to duplication of records. • Incorrect responsibilities listed for first contact based on NCFRAs HFSV Risk Profile for high risk and very high-risk jobs.	**Medium**	Changes to the CFRMIS data collection process and a review of permissions will form part of the CFRMIS Phase II Project Plan. Progress will be monitored by the Continuous Improvement Board. HFSV administration processes are reinforced within guidance and will be featured within the Cohort Training Days in 2026. The Risk Matrix will be reviewed as a result of internal audit and our case learning cycle. *Lisa Bryan – Prevention, Safeguarding & Partnerships*	01 October 2026

NCFRA Prevention 2025/26 (Cont.)

Ref	Recommendation	Priority	Management Comments	Due Date
2 (ctd)	**NCFRA should:** **1. Investigate and resolve the system auto population failures.** **2. Implement a regular gazetteer update and integration process.** **3. Implement user permission restrictions so that only the Quick Screens system can be used to created HFSV jobs.** **4. Advise all staff that HFSV jobs should be created in the Quick Screens system and not in the main database screen.** **5. Advise crews that all 116 Arson Task Force (ATF) jobs they complete should have an input in the referred by option.** **6. Advise crews that duplicate 116D direct engagement jobs should be raised with the Prevention Team to enable deletion.** **7. Review and correct the allocation of responsibilities for high and very high-risk jobs and work with the supplier to assess the feasibility of implementing automated responsibility assignment based on expected risk.** **8. Introduce periodic data integrity checks to identify and correct data issues in a timely manner.**			

We have also raised two Low priority recommendations regarding:

- NCFRA should:
    1. Define and formally document in its HFSV Policy the specific key performance indicators (KPIs) it intends to measure, monitor and report. KPIs should include:
        - % of HFSVs completed within the 42-day prescribed resolution time.
        - % of HFSVs first contact times met in accordance with the Risk Profile.
    2. Continue to report on HFSV performance, including the above KPIs, through existing governance groups.
- NCFRA should implement a system-based solution for recording and managing HFSVs that integrates HST and crew HFSV data within a single platform.

EMSOU POCA Income 2025/26

Ref	Recommendation	Priority	Management Comments	Due Date
1	We expect EMSOU to maintain full oversight of the disposal process for seized assets, ensuring that all disposals are conducted transparently and in accordance with legal requirements. Robust record-keeping should be in place to demonstrate value for money and compliance with court orders. As part of our audit, we reviewed a sample of 10 court-ordered payments made from the EMSOU account between October 2024 and July 2025. This sample included seven cash seizures and three asset disposals. We sought to confirm whether the assets were sold following the issuance of a court order and whether supporting evidence of the sale was available. Our findings are as follows: Vehicle (Court Order: 22 April 2025) This asset was involved in a joint investigation between EMSOU and Police Scotland. Although EMSOU later assumed sole control of the case, the vehicle remained stored in Scotland. Police Scotland proceeded to sell the asset via auction without notifying EMSOU, and no formal communication channels were in place to confirm the timing or legal basis of the sale. As a result, EMSOU could not confirm whether the sale occurred after the court order. Management advised that Police Scotland would need to clarify the legislative authority under which the asset was sold. We were advised that funds of £20,514.50 were received into the EMSOU account on 6 June 2025. Jewellery (Court Order: 28 August 2024) EMSOU advised that the items were sold via eBay; however, they were unable to provide the date of sale or supporting documentation. We were further advised that funds of £5,095.25 were received into the EMSOU account on 18 December 2024. Cryptocurrency (Court Order: 28 August 2024) EMSOU informed us that the asset was transferred to the Leicestershire Police KOMAINU account but could not provide the date of transfer or further details. We were advised that funds were deposited on 18 November 2024.	**Medium**	The following actions have been identified: • SOP in development to detail asset seizure and realisation, including joint operations. This will cover the methodology required for communication channels and the reconciliation of assets held in auction houses. • The officer in case (OIC) will detail all assets within the case management system.. *David Vint – Head of Economic and Cyber Crime*	31 July 2026

EMSOU POCA Income 2025/26 (Cont.)

Ref	Recommendation	Priority	Management Comments	Due Date
1 (ctd)	**The Unit should:** **1. Implement a formal process of formulating a communication channel when conducting a joint investigation with another Force to gain assurance and oversight over the sale process.** **2. Ensure that records are kept of sale to demonstrate value for money.**			

We have also raised two Low priority recommendations regarding:

- The Unit should establish a process for retaining records and evidence of asset disposal sales for auditing purposes.
- The Unit should regularly review all procedures concerning reconciliations.

EMSOU Forensics Accreditation 2025/26

We have raised one Low priority recommendation regarding:

- EMSOU-FS should develop an overarching forensic accreditation strategy or implementation plan that clearly defines the statutory and regulatory accreditation requirements the Unit is required, or intends, to comply with, and sets out how the Unit will achieve and maintain compliance.

Contact

Forvis Mazars

David Hoose
Partner
David.Hoose@mazars.co.uk

Sarah Knowles
Engagement Manager
Sarah.Knowles@mazars.co.uk

Statement of Responsibility

We take responsibility to the Office of the Police, Fire and Crime Commissioner ("OPFCC") for Northamptonshire, Northamptonshire Commissioner Fire & Rescue Authority ("NCFRA") and Northamptonshire Police ("Force") for this report which is prepared on the basis of the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

forvis mazars