**INTERNAL AUDIT RECOMMENDATIONS DASHBOARD**

**Summary of Audit Outcomes**

Audits are graded as No Assurance, Limited Assurance, Satisfactory Assurance or Significant Assurance. Some thematic audits are advisory only and not graded. Recommendations are prioritised as Priority 1 (Fundamental), Priority 2 (Significant) or Priority 3 (Housekeeping) to reflect the assessment of risk associated with the control weaknesses.

**Northants Audits**

**2023/24**

| **AUDIT** | **DATE** | **GRADE** | **RECOMMENDATIONS MADE** | | |
| --- | --- | --- | --- | --- | --- |
| **Priority 1** | **Priority 2** | **Priority 3** |
| Firearms Licensing | 21 July 2023 | Moderate Assurance | 0 | 2 | 0 |
| RUI Follow Up | 26 September 2023 | Moderate Assurance | 0 | 1 | 2 |
| Business Continuity & Emergency Planning | 01 November 2023 | Limited Assurance | 2 | 3 | 0 |
| Reasonable Adjustments Follow Up | 25 January 2024 | Moderate Assurance | 0 | 2 | 3 |
| Core Financials | 06 March 2024 | Moderate Assurance | 0 | 3 | 3 |
| Vetting | 18 March 2024 | Moderate Assurance | 0 | 1 | 2 |
| Fleet Management Follow Up | 25 April 2024 | Moderate Assurance | 0 | 0 | 3 |
| Payroll | 01 May 2024 | Moderate Assurance | 0 | 3 | 0 |
| Identity Access Management | 11 June 2024 | Limited Opinion | 0 | 5 | 1 |
| IT Asset Legacy Management | 11 June 2024 | Moderate Opinion | 0 | 2 | 3 |

**2024/25**

| **AUDIT** | **DATE** | **GRADE** | **RECOMMENDATIONS MADE** | | |
| --- | --- | --- | --- | --- | --- |
| **Priority 1** | **Priority 2** | **Priority 3** |
| Grant Funding | 27 June 2024 | Substantial Opinion | 0 | 1 | 0 |
| Medium Term Financial Planning | 18 September 2024 | Substantial Opinion | 0 | 0 | 0 |
| Asset Management | 30 October 2024 | Moderate Opinion | 0 | 1 | 3 |
| Joint Core Financials | 27 November 2024 | Moderate Opinion | 0 | 2 | 3 |
| Workforce Planning | 27 February 2025 | Moderate Opinion | 0 | 1 | 0 |

**Summary of Audit Recommendations Progress**

This table shows a summary of the progress made on new audit recommendations raised at each JIAC during the current year and annual totals for previous years where audit recommendations are still active.

| **2023/24 AUDITS** | **RECOMMENDATIONS MADE** | **RED** | **AMBER** | **YELLOW** | **GREEN** |
| --- | --- | --- | --- | --- | --- |
| Firearms Licensing | 2 | CLOSED | | | |
| RUI Follow Up | 3 | 0 | 0 | 0 | 3 |
| Business Continuity & Emergency Planning | 5 | CLOSED | | | |
| Reasonable Adjustments Follow-Up | 5 | CLOSED | | | |
| Core Financials | 6 | CLOSED | | | |
| Vetting | 3 | CLOSED | | | |
| Fleet Management Follow Up | 3 | CLOSED | | | |
| Payroll | 3 | CLOSED | | | |
| Identity Access Management | 6 | 0 | 2 | 2 | 2 |
| IT Asset Legacy Management | 5 | 0 | 1 | 0 | 4 |
| **Totals** | **41** | **0** | **3** | **2** | **36** |

| **2024/25 AUDITS** | **RECOMMENDATIONS MADE** | **RED** | **AMBER** | **YELLOW** | **GREEN** |
| --- | --- | --- | --- | --- | --- |
| Grant Funding | 1 | CLOSED | | | |
| Medium Term Financial Planning | 0 | 0 | 0 | 0 | 0 |
| Asset Management | 3 | 0 | 0 | 3 | 0 |
| Joint Core Financials | 5 | 0 | 0 | 1 | 4 |
| Workforce Planning | 1 | 0 | 0 | 1 | 0 |
| **Totals** | **10** | **0** | **0** | **5** | **5** |

**OUTSTANDING RECOMMENDATIONS**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Key to Status** |  | Action completed since last report |  | Action ongoing |  | Action ongoing with revised implementation date |  | Action outstanding and past its agreed implementation date |  | Action no longer applicable or superceded by later audit action |

**2023/24**

**RUI Follow Up – September 2023**

|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| **4.1** | **Longstanding RUIs**  *Observation:* As per the previous review, it was identified that it was necessary to prevent longstanding RUIs due to the negative effects they may present to afflicted individuals, particularly for those in the course of undergoing employment or other vetting processes. Although there has been a reduction in the number of longstanding RUIs over time, a large number of individuals still remain RUI for over one year.  Below is a summary of the status of longstanding RUIs at the time of our audits:   |  |  |  |  | | --- | --- | --- | --- | |  | | RUI 1-2 Years | RUI >2 Years | | Apr 21 | 328 | | 139 | | May 22 | 242 | | 113 | | Jun 23 | 217 | | 86 |   The responsibility for the review of longstanding RUI cases lies with Chief Inspectors, and on a quarterly basis Chief Inspectors are requested to undertake a review of longstanding RUI cases, last taking place in May 2023.  The Detective Chief Inspector now holds a meeting every week with Custody to discuss RUI cases. Additionally, RUI cases should be reviewed every 28 days by officers however this is a personal responsibility of officers and is not monitored.  We noted that the Force has the capability to actively monitor RUI figures through Niche reports that can be generated, however, these figures are not reported more widely.  *Risk*: Individuals on longstanding RUI are not treated fairly and may present a risk of reputational damage to the Force. | The Force should explore how officer’s 28-day review of RUI cases can be monitored.  The Force should actively monitor and report on longstanding RUIs to ensure that accountability and ownership is in place for individual Chief Inspectors, such as by sending RUI figures reports to a board or committee for review. | **2** | The force accepts the recommendations.  The force will consult on a standardised automation process to assist with monitoring of reviews to identify where further improvements can be made however, RUI’s have continued in a downward trend, and I am satisfied that the 28-day review process is sufficient to manage risk in the interim.  The Aged RUIs will be reviewed yearly as part of the Senior Officer Review process to drive down the numbers, and individual Chief Inspectors will be sent the data on a quarterly basis.  Governance will be via Improving Investigations Board.  Update from AR 07/08/24 - Longstanding RUI levels remain constant since 2022.  Recommendations:   * All RUI’s over 1year (315) to be reviewed, initial direction after report creation to come from OIC Supt’s to cascade and own. Then, when next feasible, long term RUI’s to be reviewed as part of the Senior Officer Review process. Officers who have failed to update/progress to be managed accordingly through the review process and line manager. * Within this recommendation I believe it to be necessary to add the review of Bail. I propose that I review all bail cases over 6months (23) to see if case remains applicable or is an admin issue. Once completed, review issues and patterns then progress to 3-6months. The necessity is that I have checked 3 cases, both need finalising with custody being updated for RUI/Bail closure and would be an easy data cleansing exercise. In addition, it would prevent legal action if we were showing an individual as under a live investigation when their case has been NFA’d. * A new report to be developed to capture total date from arrest and not just when RUI or Bail. This will provide full data on cases where a suspect has been processed as such, as at present you can have a Bail case between 3-6months and if reverted to RUI it will then go into the 0-28day list. It does not show the full picture of where are cases are being progressed. * Custody Bail Sgt to review RUI with filed occurrences, in the short-term fix to sort this as the process should be managed by the OIC and their Sgt.   Update 09/09/24 – All of the recommendations outlined above have been implemented and will be reviewed on a bi-monthly basis.  Agreed for closure at FAB 22/10/24 | 6-9 months depending on technical requirement - DCI Andy Rogers |  |

**Payroll – May 2024**

|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **Expenses are not validated or approved prior to their payment**  *Observation:* The Force's Expenses and Allowances Policy, which was last reviewed 21 January 2021 (**See recommendation 2)**, outlines that expenses will be reimbursed if the expenditure incurred in the course of duty is:   * Supported by a receipt * Of a reasonable amount * Necessary * Additional to what would have been normally spent   The policy also outlines that "Managers/ Heads of Departments and Area Commanders need only approve claims where queries are raised by the Payroll, HR or Finance functions or the claim is outside of the standard claim processes outlined within this document and require approval prior to submission.  Expenses are claimed through the Self Service Expense Claim within Forcenet. We reviewed a sample of ten expense claims made between April 2023 to August 2023 to ensure that they were legitimate, in line with the policy, authorised and paid in a timely manner. In each instance whilst we were able to confirm that payment was made in a timely manner, no evidence was provided to support the validity of each claim, or its approval.  We were advised by the Payroll Manager that expenses claims are not verified by the Payroll team, as outlined in the policy, and instead a regular audit is undertaken by the Finance Department on a sample of expenses claims to verify their validity. We conducted a walkthrough of the audit arrangements in relation to expenses and noted that there is no formalised approach to conducting the review. We were advised that each month a different expense type is focused on, with ad hoc selection of expenses claims for that month based upon instances that appear exceptional or abnormal.  We reviewed the audit log used to log and monitor expense audits and noted that the audit process consisted of requesting evidence from the individual claimant, or an explanation of the nature of the expense. None of the ten expenses selected in our sample had been audited.  As such, we note that there is no preventative control in place that approves or verifies expenses claims before they are made. We commonly see this included within a system workflow, wherein line managers must approve expenses claims prior to their processing by the payroll team.  For reference, the total expenses claimed by Officers as reported in July 2023 was £33,993, of which £5,292 related to food and subsistence and £6,849 related to mileage and parking.  *Risk:* Inappropriate expenses claims are made that are not in line with the Force's policy, and do not relate to bona fide expenses claimed whilst working on behalf of the Force. | The Force should ensure that expenses claims are formally approved and validated prior to their payment, with an audit trail retained to evidence the value and nature of the expense claimed.  The Payroll team should ensure that they receive confirmation to support the validity of expenses claims prior to their payment. | **3** | The risk of retrospective review is accepted and noted, however, the position remains that the Force’s policy is that inappropriate claims will be managed through PSD and HR and a full reimbursement would be expected. It is anticipated that with the appointment of an additional role under the Finance and Resources Officer we will be able to ensure a wider coverage and review of all claims, which will reduce the risk of those claims being unchallenged.  Update July 2024 - We now have a member of staff and undertake audits on a wider range of the expense claims which we log.   I have met recently with PSD and provide reports monthly to them.  Agreed for closure at FAB 22/10/24 | Michael Montgomery  31 March 2025 |  |
| **2** | **The Policy library includes out of date policies and procedures, and procedural guidance is not in place**  *Observation:* The Force operates a policy library which stores all the policies and procedural guidance for the organisation. This is available through the Force Intranet. We requested all policies and procedures in relation to Payroll and were provided with a number of different policies taken from the Force's policy library. We reviewed the policies provided and noted that three versions of the Expenses and Allowances, and Overpayments and Underpayments policies were available in the policy library, as well as two instances of the Overtime policy. In all cases the versions of the policies reviewed had not been reviewed in line with their review cycles, and we noted that the policy owner was not consistent across versions. In one extreme instance an Overtime Policy had an effective date of April 2007.  We raised this to the Payroll Manager during our review, who subsequently provided an updated version of the Expenses and Allowances and Overtime policies. Whilst we confirmed that the Overtime policy was last reviewed in April 2023 with a next review date of April 2024, the Expenses and Allowances policy had an effective date of June 2021, requiring review in June 2022. We were advised that the Expenses and Allowances policy was currently under review.  Additionally, we reviewed the Starter and Mover procedural guidance notes in place to support Payroll staff and confirmed that this outlined the approach for inputting starters and transferring movers within iTrent. However, we note that the Force does not have procedural notes in place which document the approach to inputting, reviewing and approving payroll related data for other common processes including leavers, deductions, and variations. At similar organisations these often utilise screenshots to illustrate the process in place, supported by commentary. We find that maintaining clearly defined procedural notes provides continuity in performing day to day processes, as well as supporting business continuity.  *Risk:*Staff are unaware of the current processes in place relating to Payroll, leading  to inappropriate claims or requests which are not aligned to the Force's policies.  Payroll staff are unaware of operational processes, leading to an inconsistent and  inappropriate approach to processing payroll data. | The Force should review the policy library to ensure that only the most up to date versions of each policy are available.  The Force should ensure that the Expenses and Allowances policy is reviewed on a timely basis, in line with its review cycle.  The Force should develop procedural guidance documents that outline the process for the input, review, and approval of Payroll related data within iTrent. Guidance should include version control to support a regular review of the process, ensuring it is reflective of current practice. | **2** | A review of the policy library by the Chief People and Finance Officers is being completed and all policies and procedures will be reviewed and where appropriate revised throughout 2024/25.  Update May 2024 - This is currently ongoing with collaboration across HR and Finance to look at updates and clarity where needed.  Update July 2024 – Discussions are ongoing in relation to this.  Update September 2024 – The Travel and Expenses Policy is currently being reviewed by SM and will be circulated for consultation once complete. The Pay and Subsistence Policy was updated in 2023 but it is still on the old template so this will be moved to the new template and reissued.  Update February 2025 - The draft policy went to FEM for consideration and was approved, this then went to full consultation within the Force and the new revised policy was implemented in January.  Agreed for closure at FAB 25/02/25 | Suzanne McMinn & Nick Alexander  31 March 2025 |  |
| **3** | **Access arrangements for iTrent are under review, and permissions are not formally reviewed on a regular basis**  *Observation:* At the commencement of the audit, we were provided with a permissions list extracted from the Force’s payroll system, iTrent. We note that this included all payroll staff as having “System Administrator” access. Subsequently, during the review the Payroll Manager provided an updated extract, which illustrated that these permissions had been reduced for payroll officers to “Payroll with HR admin”. However, through discussions with the Change Programme Manager we were advised that, as part of the ongoing integration with NCFRA, permissions were being reviewed to ensure that these are limited only to activities that are required by those staff members.  Additionally, we were advised that members of the payroll that leave the team are immediately removed from the Payroll system. We were able to confirm that a recent leaver from the Payroll team no longer had access to iTrent through review of access permissions before and after their cessation. However, we note that the Force do not formally review the permissions on a regular basis. We were advised that an annual review is undertaken of permissions within the HR system, Unit4.  *Risk:*Inappropriate access to the payroll system increases the likelihood that inappropriate payments are made, and/or fraudulent behaviour. | As planned, the Force should review access permissions within  the Payroll system, iTrent, as part of the NFCRA integration project that is ongoing. Permissions that facilitate the inputting, amending, and deletion of payroll data should be limited to Payroll staff, as well as IT and MHR consultancy related staff to facilitate the operation and update of the system.  Permissions should be developed to ensure segregation of duties is maintained.  Access permissions to iTrent should be reviewed on an annual  basis as part of the existing annual review of the Unit4 HR  system. | **2** | Alongside the system access reviews that are completed quarterly, we will ensure that payroll access is independently reviewed to ensure segregation and  appropriate scrutiny.  Update Sep 24 – Reviews are already in place. Discussion are ongoing regarding system reviews.  Agreed for closure at FAB 22/10/24 | Michael Montgomery  30 June 2024 |  |

**Identity Access Management – June 2024**

|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **Lack of Periodic User Access Reviews**  *Observation:* Regular user access reviews should assess whether the Windows Active Directory (AD) user base, responsible for managing logins, permissions, and authenticating access to associated applications, is accurate and that individuals have not been assigned unnecessary access.  A regular regimen of access reviews has not been established to determine the suitability of access privileges for Windows AD accounts.  *Risk and Impact:* Failure to implement regular access reviews can lead to individuals retaining unnecessary access to Windows AD and related systems, creating additional points of access to external attackers. | Each organisation should implement a regular (e.g. quarterly) regimen of Windows AD access reviews. Line managers should review the access of their staff and any other users such as partnership workers that they are responsible for. Any  unnecessary access detected during these reviews should be removed from relevant individuals.  As the Force is implementing SailPoint across its employees, it should assess whether SailPoint could provide this service automatically. For users not covered by SailPoint alternative  manual processes may be required proportionate to the risk. | **2** | This recommendation is broadly accepted by management as it is recognised that there are currently process in place to address this, they do not currently extend to this level of scrutiny. Therefore, although there will be oversight of this process within the annual information auditor plans and role (due to be  implemented by the end of the 2024 calendar year), this in-depth level of scrutiny will be fully implemented once we have the correct JML and access controls processes in place which will be managed automatically via the implementation of ITSM tool in December 2025. The source information reviews (a required prerequisite) will begin when the new information assurance structure is in place, this will inform the data utilised within the ITSM tool.  25/07/2024 No further update.  Update 06/09/24:  The process is currently conducted in conjunction with the Information Assurance and Systems admin teams and due to resource constraints is limited to ad hoc reviews at this time. However the new structure will facilitate the coordination of the ROPA, the underlying access required and then the audits will be planned and executed by the new information audit team.  Update 30/09/24 (YH)  Consultation and recruitment underway  Update 31/10/24 (YH)  Consultation now complete and largescale recruitment underway. DDaT are working with the comms department to facilitate an effective and targeted recruitment campaign to ensure these roles are filled.  Update 09/01/25 – No change | Trina Kightley-Jones, Head of Information  Assurance  31 December 2025 |  |
| **2** | **Multifactor Authentication for Fire AD Accounts**  *Observation:* Multifactor Authentication (MFA) provides additional layers of authentication beyond passwords, that attackers must also breach should passwords become known to them. Best practice frameworks such as Cyber Essentials recommend that MFA is applied where available, and always for cloud services.  Accounts within the Police Service Windows AD domain have MFA configured, however, the process to enable this for Fire Service AD accounts is still ongoing.  *Risk and Impact*: Should the passwords for Fire Service user accounts be determined in a security attack, such as through the use of malware, these accounts could be accessed resulting a severe security breach that could be used to access data across the network. | NCFRA should continue the process of setting up MFA for Fire  Service accounts, ensuring that all accounts are covered by this process. | **2** | We agree with the audit recommendation and acknowledge the importance of multifactor authentication for securing Fire Service accounts. As noted in the  recommendation, we have started the process of implementing this security measure for administrative accounts and on a per project basis. The intention  would be to enable this for accounts within EntraID. Full implementation will require executive support from the organisation and of other affiliated bodies.  We will commence this process, monitor the progress, and report any issues or challenges. A date has been set of 30/09/2024 subject to approval by the  organisation.  Update 13/08/2024:  In progress, delivery dates not yet amended.  Update 06/09/24:  MFA - Currently in 28 day consultation with Fire, Lisa Jackson to advise of consultation outcome.  Update 30/09/24 (YH)  Lisa Jackson in Fire has confirmed that this consultation has been agreed in Fire. However following initiation of this work and further investigation by DDaT, a paper is being developed by the Digital Security Architect to consider the wider security considerations in relation to MFA and the holistic cyber security implications. This work should not be completed in isolation and there must be precursor work regarding security keys ect prior to the switching on of MFA in fire. A request for this action to be extended to Jan 2025  Update 30/11/25 (YH)  A request for this action to be extended to Jan 2025 has been approved. YH to send reminder to ensure work is progressing at required pace.  Update January 25 - A request for this action to be extended to Jan 2025 has been approved. Digital Security Architect developing paper for approval. On track  Update January 2025 - It has been confirmed that the ECF and Union have not yet agreed on complete MFA for Fire. The SLT meeting minutes state that MFA is not mandatory in fire and the action to progress it was closed. The CAF and digital standards recommendations highlight MFA in fire as a requirement. As a result, an additional paper will be written by DDaT Digital Security Architect. **Request to move date to 30th April 2025** for this work to be completed and approved to be sought | Roy Cowper, Enterprise Architect  30 September 2024  January 2025  30 April 2025 |  |
| **3** | **Privileged Access**  *Observation:* Privileged Identity Management (PIM) should, according to the time-restricted access policy configured in the PIM tool, provision privileged roles to individual users for a specified period before being withdrawn automatically.  Within the Police Azure tenant access to privileged accounts is controlled on a timerestricted basis, with higher privileges being assigned for shorter periods of time. While some low-level privileges are assigned to users permanently this has not been viewed as a risk due to their extremely limited capabilities. Within the Fire Azure tenant a similar system has been implemented, however time-restricted access has not yet been applied as strictly, with some medium-level privileges being assigned to a number of fire user accounts permanently. We were informed by management that such privileges should only be provided on a time limited basis and thus require review.  *Risk and Impact:*Privileges assigned to accounts on a permanent basis may be used to apply unapproved changes without management oversight. | Each organisation should align the privileged access management  procedures to ensure that where possible a principle of least privileged is followed when assigning access to user accounts.  Privileges assigned to users on a permanent basis, such as those assigned to users in the Fire Service Azure tenant should be  reviewed and if possible, removed, such that they can be  reassigned on a temporary basis to apply specific authorised changes. | **2** | We acknowledge the audit action and agree that privileged access management is a key aspect of ensuring cybersecurity. We have reviewed the privileges assigned to users in the Fire Service Azure tenant and some work has already been completed to bring key AzureAD roles under the control of PIM. We have removed permanent privileges that didn’t require escalation and established a process for requesting and granting them on a temporary basis when needed. The process of bringing the Fire tenant up to the same level as the Police tenant in respect of this security control will continue as part of business as usual. A date has been set of 30/09/2024.  25/07/2024 No further update.  Update 30/09/24 (YH)  Review now complete and draft policy disseminated ahead of consultation process. Change request also submitted by EA to ensure delivery of recommendations highlighted in policy fully. Policy restricted at this time but shared with VA and PB. Recommended for closure.  Agreed for closure at FAB 22/10/24 | Roy Cowper, Enterprise Architect  30 September 2024 |  |
| **4** | **Password Management Tool Implementation**  *Observation:* It is good practice to use a password management tool to secure the passwords for generic  administration and service accounts in order to prevent their exposure through the use of less secure password storage methods.  A password management tool has not been implemented for Police Service AD service accounts, whilst for Fire Service accounts a tool has been implemented but which only contains passwords for a small minority of accounts.  *Risk and Impact:* Passwords may be documented in insecure locations such access to relevant accounts  may be achieved the event of a security breach*.* | Each organisation should store all generic administration and  service account passwords in a password management tool. | **2** | This recommendation is accepted and there is a PAM (Password Access Management) Project in progress that is being led by the Transformation and Change team with a project manager assigned. Budget has been allocated and we have collated requirements which include the ability to store all generic administration and service account passwords, and supplier demonstrations have now taken place. This will be reviewed bi- monthly to ensure progress is made.  Update 25/07/2024 VS:  All requirements are done and quotes obtained, and business case is in development.  Update 30/09/24 (YH)  Currently in the commercial process for signing by the commissioner.  Update January 2025 - The commercial activity has been placed on hold – Queries relating to Cloud viability now being explored as requested by stakeholders | Andrew Jones, Head of Transformation and  Change  31 March 2025 |  |
| **5** | **Completion of Access Changes**  *Observation:* Changes to access should only occur on supply of a proper request.  The OPFCC, Force and NCFRA were unable to provide relevant documentation to support the completion of access changes as follows:   * For five out of eight joiners, a HR notification form was not available. * For one out of eight joiners, evidence of vetting and training was not available. * For all eight leavers, a HR notification form was not available.   *Risk and Impact:* User accounts may be created or disabled without proper justification. | Emails and other documents supporting access requests should be automatically attached to tickets raised to the service desk. If this is not feasible the access management procedures followed  by the service desk should state that all such emails/documents  should be manually attached to relevant tickets and relevant staff made aware of this requirement | **2** | This recommendation has been reviewed and has been accepted. Although tickets are already created from HR data, this process will now be reviewed to identify the capability of the current HR hub, ITSM tool and automation, if that cannot be easily done within these existing platforms then this will be developed with the new ITSM tool. The associated action will be to review this and report to key stakeholders.  Update 11/07/2024 DC:  The ITSM procurement phase is well underway, due for completion August/September 2024.  Update 24/07 DC - We have undertaken a review of the capabilities of both ITSM Police and Fire ITSM solutions and neither have the ability to manage access requests in the method described.  We are in the process of procuring a new ITSM joint platform, the procurement process is due for completion next month, where we will work with the supplier to understand if the data we receive from HR in the JML process can be used to provide both organisations with a higher level of audit capability in this area.  The new ITSM platform is unlikely to be made live until the next financial year.  Update 13/08/2024 (YH)  Discussed with CDO as procurement is still ongoing and implementation likely to be Autumn 24. Request to adjust delivery dates in line with ITSM revised implementation.  Update 06/09/24: (YH) Due to procurement activity and delayed ITSM implementation request for these dates to move to March 2025  Update 31/10/24 (YH)  The procurement for the tool is progressing well. The revised project stage gates remain accurate.  Update January 25 – No change | Dan Cooper, Head of Technical Support  01 July 2024  December 2024  31 March 2025 |  |
| **6** | **Monitoring and Logging Policy**  *Observation:* A specific IT policy should set out the organisational requirements for monitoring and logging, this should be used to guide the operations of the IT team as well as to inform regular users of any responsibilities regarding the monitoring and logging process.  A specific monitoring and logging policy detailing requirements and procedures for access monitoring and information logging has not been developed. Some requirements, such as the logging of multiple failed password attempts, have been added to the information security / access control policies, however no unified monitoring and logging policy / section has been implemented.  *Risk and Impact:* Inconsistencies in employees’ understanding of their roles and responsibilities in regard to monitoring and logging as well as a failure to perform their required tasks. Failure to perform these tasks may reduce the detection rates of security incidents which could lead to reputational damage. | Each organisation should devise a monitoring and logging policy,  including necessary ownership, version control and review sections. Once approved it should be communicated to those individuals that perform security monitoring and configure security  logs. | **3** | We agree with the audit action and recognise the importance of having a clear and updated policy for monitoring and logging. We will allocate a task to  develop a draft policy that defines the objectives, scope, roles and responsibilities, frequency, and procedures for monitoring and logging.  25/07/2024 No further update.  Update 06/09/24:  Logging and Monitoring Policy (Identity Access) is not the same as the IT Asset Management Policy (IT Asset Legacy Management). On track, this policy is in development and is being written by Simon Creasey (Digital Security Architect), draft to be shared by the end of the month.  Update 30/09/24 (YH)  Draft policy completed and disseminated for review. Request by security architect for policy to be restricted. Copies shared with VA and PB. Recommended for closure.  Agreed for closure at FAB 22/10/24 | Roy Cowper, Enterprise Architect  30 September 2024 |  |

**IT Asset Legacy Management – June 2024**

|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **Automated scanning of hardware and software is not used to identify inaccuracies in the IT asset register.**  *Observation:* Automated scanning of hardware and software enables organisations to identify discrepancies between the IT asset register and devices present on their network.  The Head of Digital, Data and Technology confirmed that there is currently no software in place to scan the network for discrepancies between the IT Asset Register and the actual devices deployed across the Force. Northamptonshire Police & Fire are currently in the process of purchasing a new IT Service Management (ITSM) tool, which we are informed will include this function, with the intention to begin implementation from May 2024.  Furthermore, dependent on their type, most devices are separately managed by other software; for example, laptops are registered by Intune, however apart from a historic feed from the Blackberry management software for mobile devices, there are no other automated updates to the IT asset register to keep it updated.  *Risk and Impact:* Inaccuracies in the IT asset register, such as those that arise from failure to apply manual updates of new devices, prevent effective management of the Northamptonshire Police & Fire devices, whether this be from a financial, security or service management perspective. | Continue with the planned implementation of a new ITSM tool that includes device scanning to identify discrepancies with the IT Asset Register.  Once implemented the software should also consume feeds from  the management software for each class of device.  IT asset register discrepancies identified by automated scanning  or following receipt of information from device management software should be investigated before their application to the IT  asset register | **2** | The procurement and implementation of the new ITSM tool is ongoing and DDaT will implement the software in three phases, starting from the first quarter of the current fiscal year and ending by the fourth quarter of the next fiscal year.  The first phase will involve installing and configuring the software on the servers and integrating it with the existing IT systems.  The second phase will involve testing and validating the software functionality and performance, as well as training the staff on how to use it. The third phase will involve deploying the software to all the devices and conducting a post- implementation review.  The current system does not provide Integrations required to consume feeds, however these capabilities are present in the new tool.  In the meantime, we are currently exploring opportunities to see how the reporting tools can help us determine device usage. The initial goal is to identify devices not in use against our asset lists.  Update 11/07/2024 DC:  The ITSM procurement phase is well underway, due for completion August/September 2024.  Update 13/08/2024 (YH)  Discussed with CDO as procurement is still ongoing and implementation likely to be March 2025. Request to adjust delivery dates in line with ITSM revised implementation.  Update 30/09/24 (YH)  Request to move dates accepted.  Update January 25 – No change - On track. | Dan Cooper, Head of Technical Support -  DDaT  31 December 2025  December 2024  31 March 2025 |  |
| **3** | **Assessments of IT infrastructure risks are performed on an ad-hoc basis**  *Observation:* IT infrastructure should be subject to formal periodic review to assess its adequacy and highlight any risks that are not identified through day-to-day management activities.  We noted periodic assessments of the infrastructure do not take place, instead risks are identified in the course of normal management activities. We found only three  risks relating to infrastructure support had been identified and assessed, with these risks covering software upgrades, Cyber Security and ageing systems, and hardware and software coming towards their end of life.  *Risk and Impact:* The IT Infrastructure does not support the future needs of the force or carries unidentified risks that threaten the availability and security of IT systems | Periodically assess the adequacy of IT architecture to identify and  locate potential risks. | **3** | DDaT accept the recommendation. The Enterprise Architecture team are in the process of developing a suite of roadmaps. The infrastructure roadmap  was developed in late 2023 and is designed to account for a number of identified risks. These risks will be captured in the register more formally going forward. These risks will the then be managed in line with our existing risk management processes.  In addition, we are about to enter a procurement process for an Enterprise Architecture tool that will bring together all the information from multiple sources  inclusive of risks, contract end dates, the solution / software catalogue and infrastructure components to enable better visibility of the IT Landscape.  25/07/2024 No further update.  Update 30/09/24 (YH)  Full review complete. The IT infrastructure roadmap is based upon all the current infrastructure for both organisations and the requirement to update particular technology areas. The risks that this roadmap looked to mitigate have now been identified and put forward to the CDO board and as a result here multiple pieces of work now exist in the portfolio tool and these will address the risks. These risk are highlight as originated from EA risks but are managed within the wider DDaT technical debt / aging system risk. The roadmap is a signed off working document. Recommended for closure.  Agreed for closure at FAB 22/10/24 | Roy Cowper, Enterprise Architect – DDaT  31 December 2024 |  |
| **5** | **A formal IT Asset Management policy/procedure document has not yet been implemented.**  *Observation:* An IT asset management policy is necessary for appropriate governance of IT assets  acquired and managed by the Force.  By enquiry with management, we noted that an IT Asset Management Policy is being drafted but has not yet been released to staff. Management are looking to implement the policy from April 2024.  *Risk and Impact:* Confusion in the effective management of IT assets and failure to track assets effectively, potentially leading to unnecessary procurement of IT assets and failure to effectively manage IT assets omitted from the IT asset register*.* | As planned, publish an IT Asset Management policy setting out  policy statements related to each stage in the IT asset lifecycle. | **3** | We agree with this recommendation and have initiated the process of developing an IT Asset Management policy that covers all the stages of the IT asset lifecycle, from planning and acquisition to disposal and decommissioning.  The draft IT Asset Management policy is currently under review by the senior management team.  Update 11/07/2024 DC:  The draft policy is under review by the CDO.  Update 24/07/24 - An updated IT Asset Management policy has been through a first draft and is on a second re-write, looking to condense other policies pertaining to IT asset management, such as IT Equipment Disposal and Removeable Media Policies. I’ll begin to work on the next draft after my leave, returning 12th August, for resubmission to the CDO in preparation for the September CDO Board.  Update 06/09/24:  Approval in Fire needed. This will go to CDO board in Sept, then it will go to Fire for consultation process. Fire have a specific format.  Update 30/09/24 (YH)  Shared at the CDO board in September for approval. Will now be sent to fire to begin consultation process. As a result, dates will need to adjusted to ensure this process is undertaken before publishing. Request to amend dates to 30/11/24.  Update 30/11/24 (YH)  A draft policy has been agreed By CDO. DC had been in discussion with Fire re formatting which has now been agreed. Policy to be formally submitted to fire W/C 11/11 to go through governance  - date amended to 31/01/2025.  Update January 25 - Policy written and added to template; confirmed as being appropriate by BS. EWIA for the policy with fire for additional review from disability networks to ensure it won’t cause concern. Once the EWIA is approved it will be passed into a formal consultation which will take 28 days. (DC)  Approved for closure at FAB 25/02/25 | Dan Cooper, Head of Technical Support -  DDaT  30 June 2024  30 September 2024  30 November 2024  31 January 2025  Complete |  |

**2024/25**

**Grant Funding – 27 June 2024**

|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **Process of monitoring grant funding provided to grantees**  *Observation:* In the blue-light sector, it is best practice for grantees use of grant funding from the grantor to be monitored formally through quarterly monitoring reports where the grantee provides information andevidence on how funds have been spent to enable the grantor to check that grant funding has been spent in line with the funding agreement.  Monitoring arrangements should be clearly set out in funding agreements and the OPFCC should be proactive to collect monitoring information from grantees to enable early detection of instances where the grant funding has not been spent in line with agreements, including recovering any unspent funds from the grantee.  At Northamptonshire OPFCC, grant funding agreements state that “the beneficiary shall provide information requested in the format and within the timescales as the OPFCC reasonably requests from time to time.” Operationally, the OPFCC expects grantees to provide completed monitoring forms, attached with receipts and invoices as evidence of purchases made with grant funding, in Q1 of the following financial year (June 2024).  This poses the risk that the OPFCC does not obtain timely internal assurance that grant funding provided to grantees is being spent in line with grant agreements and approved grant applications, such as inappropriate purchases are being made or grantees spending is not sufficiently allocated across the timeline of the project. Also, this may cause issues in the OPFCC recovering unspent funding from grantees in a timely manner.  Additionally, we reviewed a sample of five grantees who have already provided monitoring reports and noted the following:  • One instance (Basketball Northants) where the monitoring form completed by the grantee and provided to the OPFCC does not include the required evidence of receipts and invoices for purchases made by grantee with grant funding (£6000).  • One instance (South Northants Youth Engagement) where the grantee has provided their own format of a monitoring report which is not in line withthe OPFCC required monitoring form and does not include the required receipts and invoices to evidence the grant funding spend (£3000).  *Risk and Impact:* The OPFCC’s grantee monitoring process lacks timely collection of monitoring information from grantees which could lead to the OPFCC failing to identify, in a timely manner, any instances of grantee non-compliance with funding agreements.  Grantees do not provide the required monitoring information in monitoring reports, including receipts and invoices for purchases made, which could lead to the OPFCC being unable to validate that purchases made are in line with funding agreements and recover, in a timely fashion, any underspend of grant funding from grantees. | Northamptonshire OPFCC should:   * Clearly set out and establish in funding agreements a quantifiable frequency for monitoring arrangements of grantees. * Consider more frequent monitoring processes, such as quarterly monitoring forms or using the expected outcomes and target dates in grantee applications, to enable scrutiny of, and timely internal assurance over, the use of grand funding by grantees. This will be particularly useful for larger funding provided to projects taking place over a longer period of time. * Remind grantees submitting monitoring forms that they are to be completed via the official OPFCC monitoring form and all receipts and invoices for purchases made must be attached to evidence grant funding spend. | **2** | It is pleasing to see that there are strong processes in place around this part of our business and a programme of work will be put into place to deliver against the recommendation.  Update 14/02/25 – All changes are now in place. | Paul Fell, Director of Delivery, OPFCC  30 September 2024 |  |

**Asset Management – 30 October 2024**

|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **Lack of equipment and inventory checks**  *Observation:* The Force and the Service should ensure that regular equipment inventories are taken to ensure operational readiness, to ensure that all the necessary equipment is available and in proper working conditions in preparation for an emergency.  We noted that the Force does not operate a system which allows it to check the equipment that 'belongs' in a vehicle. We reviewed the 'Occupational Driving Policy’ and noted that it is the police officer’s responsibility to ensure that the appropriate equipment is held in the vehicle, which should be checked daily. We noted that there is no auditable trail that can be evidenced to show that equipment checks are being completed.  We reviewed a sample of 10 vehicles to ensure that the appropriate equipment was in the vehicle. We used the ‘Vehicle Safety Inspection and Equipment Checklist', and matched this to the relevant department to ensure that the correct equipment is carried on the vehicle. We were not able to inspect four vehicles as the vehicles were out, however for the other six we noted that three vehicles did not have the correct equipment.  During our review of equipment management of the Service, we noted that barcodes for equipment are important in ensuring that the correct piece of equipment is checked out to the correct pump on the Redkite system. We identified that for five out of 57 pieces of equipment that was reviewed, there were no barcodes. After discussions with the firefighters, we noted that there is some difficulty in raising a defect in the redkite system if there is no barcode on the equipment.  We noted that the full inventory checks of the pump should be carried out on a weekly basis, however we identified that weekly checks had not been noted on Redkite for four pumps and we could not confirm that weekly checks had been completed.  *Risk and Impact:* Incorrect equipment may result in a lack of readiness in emergency situations. | The Force should ensure that inventory checks are carried out daily (or as suggested in the policy) and that an auditable trail is kept to evidence that inventory checks are completed.  The Service should ensure that all equipment is barcoded where appropriate to allow for effective and efficient inventory checks. | **2** | The organisations will need to implement a new system to support the ongoing management of the equipment within operational fleet. A project mandate shall now be submitted to support the commencement of a new programme of work to implement a new system. The timeline for delivery shall then be determined by the project portfolio capacity, the data cleansing and the procurement process. | Leanne Hanson Chief Asset Officer  30 November 2025 |  |
| **2** | **Lack of updated policies and procedures**  *Observation:* An asset management policy and procedural document allows for resource optimisation, accountability, maintenance planning and ensuring equipment safety.  A review of policies, process and guidance documents highlighted that the Service’s Asset Management Guidance document was from March 2020 and did not appear to have been reviewed.  Additionally, we were informed by the Head of Transport and Travel and the Chief Asset Officer that there were other policy and procedure documents that were currently out of date, and they are currently in the process of update and review.  *Risk and Impact:* The OPCC, Force and Service do not achieve their objectives regarding Fleet / Asset Management and more widely across medium/long term objectives. | The Force and the Service should ensure that policy and procedural documents for Asset Management are updated and shared with the staff members, including the Service’s Asset Management Guidance document. | **3** | The Department is currently undergoing a review and potential restructure. As part of this work is also being undertaken to establish a single Asset Strategy. This shall be aligned to the revised organisational Strategies and Plans. Linked to this will then be a full review of all Policies and Procedures to take into account the revised delivery model | Leanne Hanson Chief Asset Officer  30 September 2025 |  |
| **3** | **Lack of equipment testing**  *Observation:* Equipment testing across the Force and the Service allows for operational readiness to ensure that vehicles and equipment are ready for duty in case of an emergency.  We noted at the Force that equipment is 'tested' if required when the police officer does the equipment checks on the car, however we noted that there was no auditable trail for equipment checks therefore cannot confirm that the checks are happening daily as per the guidance in the 'Occupational Driving Policy.  *Risk and Impact:* Lack of safe equipment may compromise The Force's ability to respond effectively in the event of an emergency. | The Force should ensure that equipment testing is carried out where appropriate, and include guidance for officers within procedural documents, as well as keeping an audit trail of this | **3** | The organisations will need to implement a new system to support the ongoing management and testing of the equipment within operational fleet. A project mandate shall now be submitted to support the commencement of a new programme of work to implement a new system. The timeline for delivery shall then be determined by the project portfolio capacity, the data cleansing and the procurement process | Leanne Hanson Chief Asset Officer  30 November 2025 |  |

**Joint Core Financials – 27 November 2024**

|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| **2** | **Debt recovery**  *Observation:* The Force and NCFRA have an Aged Debt Process document in place last reviewed May 2023 which sets out the processes to be followed by Finance Operations for the collection and recovery of overdue income:   * Day 1 – A copy of the invoice is emailed out to the customer requesting a * payment date. * Day 7 – Follow up by emailing a statement to the customer. * Day 10 – Contact the customer by phone to request a payment date.   Customers are expected to be continued to be contacted at this point if no replies are received.  Additionally, a customer aged debt report is run on a monthly basis and reviewed by the Finance Operations Team Leader to determine actions to take in respect of  chasing or if debt should be forwarded to Legal or requested to be written off.  Our review of the Aged Debt Process document did find that it was due for review in August 2024, but this had not been completed at the time of the audit.  Also, we reviewed a sample of 10 debtor invoices at the Force and seven at NCFRA to confirm that aged debt processes had been followed in accordance with the  procedural document. We found:   * Force – Four instances where debt procedures had not been followed in accordance with the Process document. This included one salary overpayment (£2,400) and three other debtors (£104,419.78, £7,000 and £2828.57) where required contact at day seven, day ten and subsequent reminders had either not occurred or documented evidence could not be provided. (Range of 43 – 340 days overdue and average of 155 days). * NCFRA – Three instances where debt had now been paid, although they were late by 122 days, 111 days and 46 days from the payment date. This was due to no Purchase Order being included on the sales invoice and a lack of aged debt processes being followed. * NCFRA – Four instances where debt remained overdue and the required debt management processes had not been followed or documented evidence could not be provided per the Process document. In addition, two of these instances have been further delayed due to invoices being as there is no Purchase Order.   *Risk and Impact:* Aged debt processes are not followed or performed in a timely manner leading to loss of money owed to the OPFCC.  Purchase orders are not included on Sales Invoices when required resulting in a build of overdue income and delayed payments to the OPFCC. | 1. The Force and NCFRA should review the Aged Debt Process document in line with its review cycle. 2. The Force and NCFRA should ensure that the Aged Debt Process is followed in a timely manner for overdue income and documented evidence is retained. To do this there should be sufficient oversight within the Finance Team of overdue income and clear escalation procedures in place to ensure debts are chased in accordance with timelines in the Aged Debt Process. 3. NCFRA should ensure that Purchase Orders are included on Sales Invoices when required, identifying customers that require this and communicating this to the relevant staff to avoid payment delays. | **2** | With the centralisation of raising of sales invoices, the team will have the ability to influence and control the process from start to finish. This will ensure completeness of data before the debt is due for chasing removing delays in payment.  As part of the centralisation process, it will also ensure consistency of process so that people are not new to processes and do not miss or overlooked aspects such as contact information and then consistent chasing and management is continued.  The aged debt process has been reviewed, and alerts set up that the policy is due a further review at its appropriate date. Cross training has been carried out on the aged debt process over the whole department offering resilience and awareness.  Update – This has now been communicated with the SIT and the internal process resolved. | Annie Blake – Finance Operations Team  Leader, Nat Freeman – Head of Finance.  01 January 2025 |  |
| **5** | **Credit notes**  *Observation*: A credit note is usually raised by a service request or email request and approved by a different member of the Finance Operations Team. After approval and once an invoice reference has been entered, the credit note should automatically match to the paid invoice on the system to complete a timely payment.  We reviewed a sample of ten credit notes at the Force and NCFRA and noted one instance at the Force where the credit note had failed the automatic matching  process, and the credit remain unpaid (£54.79) since April 2024.  We were advised by management that this has been raised with the Support Team to who are still investigating the issue.  *Risk and Impact:* The Force are unaware of system issues that could lead to further credit note matching issues and delays in payments to customers. | The Force should continue to investigate the issue and seek a  timely resolution. Once the issue is identified the Force should  consider additional preventative controls, such as systemic controls, that avoid the matching process failure from occurring again | **3** | Credit notes will be completed within the finance operations team. A request will be made via a service request and then entered into Unit 4. Investigations into Unit 4 and automatic matching will continue.  Training has been carried out across the team for awareness | Finance Operations Team  01 March 2025 |  |

**Workforce Planning – 27 February 2025 2024**

|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **No formal succession plans for critical roles**  *Observation:* We confirmed an exercise had been undertaken to identify critical roles across police officers and staff. We were provided with a spreadsheet which mapped each role into the following categories:   * Tier 1: Core operational function * Tier 2: Critical support to operational function * Tier 3: Non-critical support to operational function   However, management advised that formal succession plans had not been put into place for the core or critical roles identified, to ensure establishment stability and continuity of service, manage career pathways, and identify and place high potential staff in leadership roles.  *Risk and Impact:* Key roles are not identified, and succession plans are not developed to ensure continuity of service. Therefore, the Force is unable to fill key roles sufficiently quickly, leading to operational deficiency. | The Force should develop formal succession plans for critical roles to establish the dependencies of each role, the role specification, potential successors in emergency, short/medium/long term, and the handover processes should a key member of staff leave at short notice.   * Dependencies of each role such as key skills, competencies and qualifications. * The role specification. * Individuals with potential to assume critical roles in emergency, short term, medium term or long-term capacity; and, * Handover processes should a key member of staff leave at short notice.   Succession plans should be periodically reviewed to ensure they are accurate and up to date | **2** | Liaison with Workforce Planning to identify critical roles. Work on going to look at skills for critical roles and how individuals can identify their current skill set and identify any development required. Looking at utilising about me section on Talent Tile of PDR and to utilise the Talent Tile to produce talent pools which indicate when individuals would be ready for role e.g. ready now/short/medium or long term | Caroline Oppido  01/09/2025 |  |

**Regional Collaboration Audits**

**2023/24**

| **AUDIT** | **DATE** | **GRADE** | **RECOMMENDATIONS MADE** | | |
| --- | --- | --- | --- | --- | --- |
| **Priority 1** | **Priority 2** | **Priority 3** |
| EMSOU – Capital Programme | March 2024 | Moderate Assurance | 0 | 2 | 0 |
| EMSOU – HMICFRS Action Plan | May 2024 | Moderate Assurance | 0 | 1 | 0 |

**2023/24**

**EMSOU – Capital Programme March 2024**

|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **Funding of EMSOU Capital Programme**  EMSOU produces a Capital Programme each year as part of the budget setting process, which covers the budget for the upcoming year and a forecast budget for the following 3 years. This covers the expenditure from replacement of assets and the funding from grants, reserves and additional revenue contributions. Funding is then agreed at the PCC/CCs meeting, following recommendation from the CFO/FDs Board, as revenue funding from the Force for the upcoming year in their budgets.  Audit has reviewed the current Capital Programme and noted that reserves will be fully utilised by 2024/25 and therefore further funding will be required from the Forces.  HMICFRS have also found areas of concern in their PEEL 2021/22 review into Serious and Organised Crime. This noted concerns regarding the funding model for EMSOU as the PCC/CCs meeting couldn't agree on a three-year settlement, therefore leaving the Unit with the uncertainty of yearly funding.  *Risk and Impact:* The Unit is not able to replace or maintain current capital assets and is unable to fund the purchase of new capital assets. | The Forces and Unit should develop a Capital Programme to ensure that any future deficits in capital funding can be met. This should align to HM Treasury's three-year funding formula for serious and organised crime.  . | **2** | A revised Capital Programme will be produced that reflects the future Target Operating Model for the Unit and updated to include any future replacement costs for covert/control room equipment.  The Capital Programme will consider the funding requirement, funding options and guidance on any accounting arrangements – this will be built into funding discussions with CFO/FDs and reported back to the regional CC/PCCs Board.  Update – Sept 2024  The Regional CFO’s met in March 2024 and agreed the 4 year Regional Capital Programme, recognising the current Target Operating Model review could result in a requirement to refresh the programme. The CFO’s agreed to fund the regional capital plan for 2024/25, recognising the asset replacement reserve is expected to be fully spent this financial year.  The most appropriate method of contribution to the capital programme was also discussed and the CFO’s agreed to the full contribution to be made by each force during the year and any underspends, to be retained in the regional asset replacement reserve. | EMSOU Head of Finance and Corporate  Services  30 September 2024 – subject to regional agreement on the Target  Operating Model |  |
| **2** | **Multiple Fleet Management Approaches**  The Unit uses around 150 vehicles, with about half managed by EMSOU while the remainder are managed by one of the five Forces.  This has resulted in different procurement and replacement strategies for the Unit's Fleet - a point that has been raised as part of the HMICFRS' review into EMSOU as part of the PEEL 2021/22 regional reviews into serious and organised crime. This  identified a cause for concern where it would be more efficient to have a single capital replacement strategy and budget for the Unit, also allowing for savings to be made by adopting a regional approach to the procurement of vehicles and equipment.  *Risk and Impact*: Vehicles used by EMSOU are not appropriately maintained and/or replaced, increasing the risk of injury and/or death to the public, officers and staff. | The Unit should adopt a single fleet management approach to procurement and replacement of vehicles | **2** | A review of the fleet replacement process will be undertaken to consider any alternative procurement arrangements and whether this would deliver improvement in relation to:   * Purchase cost of vehicles * Service and maintenance arrangements * Fleet admin processes.   Update – Sept 2024  Following consultation with the Regional Fleet Managers and the Regional CFO’s, it was confirmed that all 5 forces are on the same procurement framework and that no direct savings would be realised by moving to a single lead force for the purchasing of vehicles. Costings presented showed that moving to a single lead force procurement model would create additional demand on the designated lead force which would be proportionally more expensive than the current arrangements. It was therefore decided to continue with the current procurement model.  The forces have agreed for EMSOU to work with the Regional Fleet Managers to review existing processes to identify efficiencies, reduce bureaucracy and where possible adopt consistent processes/methodologies. The areas identified for review are as follow:   * + Service requirements and safety checks   + Repairs and maintenance of vehicles   + Trigger points for vehicle reviews   + Covert vehicle blue light and radio fitments \*HMIC recommendation\*   + Road traffic accident that occurs due to the presence of a police vehicle (POLAC) * Information regarding new starters driving standards is not automatically provided, resulting in a risk to officers and members of the public, as managers are not able to suitably manage their officers training requirements. | EMSOU Head of Finance and Corporate  Services  30 September 2024 |  |

**EMSOU – HMICFRS Action Plan May 2024**

|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **Strategic Governance Board ToR**  ToR are used to define the aims, methods and reporting for key governance forums.  These are essential documents that, alongside the wider governance framework, ensure an effective regime of oversight and review.  Audit has reviewed the ToR for the Strategic Governance Board and found several items of key information not included, such as:   * attendees and roles. * frequency of meetings. * standing agenda items. * reporting and escalation.   *Risk and Impact:* Forums relating to workforce planning are not held regularly enough, with appropriate seniority, covering key areas or with appropriate reporting. | The Unit should update the ToR for the Strategic Governance  Board and Performance Management Group to include all key information, including:   * frequency of meetings. * attendees. * who chairs the meeting and relevant deputies. * standing agenda items. * where the board reports to and where they receive reports from.   . | **2** | A review of the terms of reference and governance structures in EMSOU are being reviewed as part of the implementation and review of The Operating  Model. A new Terms of Reference template has been generated for all meetings within EMSOU to ensure consistency, strategic direction and governance in line with all priorities. The Terms of Reference for the Strategic Governance Board will be refreshed in line with the new format which includes the noted information in this report.  Update - Ongoing as part of the Target Operating Model project.  Update - Sept 24  The Terms of Reference have been updated. | T/ DCS Nick Waldram (Head of EMSOU)  03 May 2024 |  |