**INTERNAL AUDIT RECOMMENDATIONS DASHBOARD**

**Summary of Audit Outcomes Audits** **for Mazars (from 2023/24)**

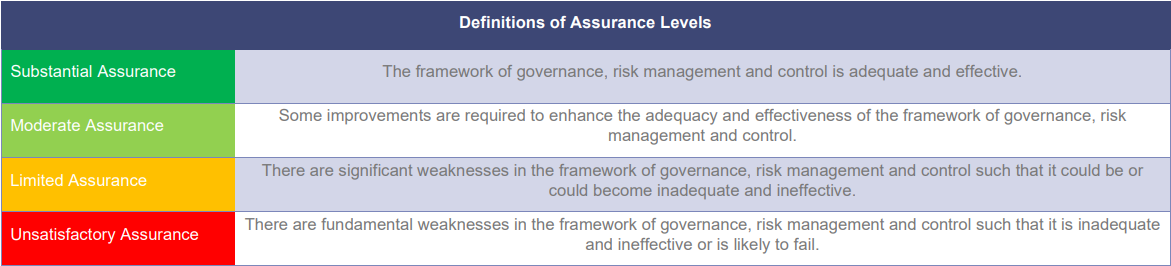
Audits are graded as Unsatisfactory Assurance, Limited Assurance, Moderate Assurance or Substantial Assurance.

Recommendations are prioritised as High Priority, Medium Priority or Low Priority to reflect the assessment of risk associated with the control weaknesses.

| **AUDIT 23/24** | **DATE** | **Assurance levels** | **Agreed Action plans** | | |
| --- | --- | --- | --- | --- | --- |
| **High** | **Medium** | **Low** |
| Risk management | Jan 2024 | Moderate | 0 | 8 | 2 |
| Core Financials | March 2024 | Moderate | 0 | 3 | 3 |
| Grievance | March 2024 | Substantial | 0 | 0 | 1 |
| Payroll | April 2024 | Moderate | 0 | 3 | 1 |
| EDI | May 2024 | Moderate | 0 | 2 | 2 |
| New systems Assurance | May 2024 | Moderate | 0 | 2 | 0 |
| Identity Access Management | June 2024 | Limited | 0 | 5 | 1 |
| IT Asset Legacy Management | June 2024 | Moderate | 0 | 2 | 3 |

| **AUDIT 24/25** | **DATE** | **Assurance levels** | **Agreed Action plans** | | |
| --- | --- | --- | --- | --- | --- |
| **High** | **Medium** | **Low** |
| Safeguarding | Sept 2024 | Limited | 1 | 5 | 1 |
| Asset Management | Oct 2024 | Moderate | 0 | 1 | 3 |
| Core financials (Joint) | Nov 2024 | Moderate | 0 | 2 | 3 |
| Payroll | Feb 2025 | Substantial | 0 | 1 | 0 |
| Succession Planning and Promotions | June 2025 | Moderate | 0 | 1 | 1 |

A screenshot of a computer screen

Description automatically generated

**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.

| **2022/23 AUDITS** | **RECOMMENDATIONS MADE** | **Essential** | **Important** | **Standard** |
| --- | --- | --- | --- | --- |
| Safeguarding Policy & Procedures | 7 | Closed | | |
| Organisational Governance – Core Code of Ethics | 3 | Closed | | |
| MTFP & Budget Management | 2 | Closed | | |
| Financial control environment | 0 | N/A | | |
| Payroll | 6 | Closed | | |
| AP/AR | 3 | Closed | | |
| Project Management | 2 | **Closed** | | |
| People Data | 2 | Closed | | |
| Contract Management | 7 | Closed | | |
| TOM – Performance Management | 1 | Closed | | |
| ICT Network Infrastructure Security – Windows fileserver | 2 | Closed | | |
| ICT Privileged Access Control | 2 | Closed | | |
| **Totals** | **37** | **0** | | |

| **2023/24 AUDITS** | **RECOMMENDATIONS MADE** | **High** | **Medium** | **Low** |
| --- | --- | --- | --- | --- |
| Risk management | 10 actions from 3 recs | 0 | 2 open  **1 closed** | **Closed** |
| Core Financials | 6 | Closed | | |
| Grievance | 1 | 0 | 0 | **Closed** |
| Payroll | 4 | 0 | Closed | **Closed** |
| EDI | 4 | Closed | | |
| New systems Assurance | 2 | Closed | | |
| Identity Access Management | 6 | 0 | 4 | Closed |
| IT Asset Legacy Management | 5 | 0 | 1 | 1 |
| **Totals** | **38** | **0** | **7** | **1** |

| **2024/25 AUDITS** | **RECOMMENDATIONS MADE** | **High** | **Medium** | **Low** |
| --- | --- | --- | --- | --- |
| Safeguarding | 7 | **Closed** | **Closed** | **Closed** |
| Asset Management (Joint) | 4 | 0 | 1 | 3 |
| Core financials (Joint) | 5 | 0 | **Closed** | **Closed** |
| Payroll | 1 | 0 | 1 | 0 |
| Succession Planning and Promotions | 2 | 0 | 1 | **Closed** |
| **Totals** | **19** | **0** | **3** | **3** |

**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 superseded by later audit action |

**2022/2023**

**Project Management – May 2023**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Issue** | **Recommendation** | **Management Comments** | **Priority** | **Officer Responsible** | **Timescale** | **Status** |
| **1** | |  | | --- | | **Weakness**  The level of the Competency Based Training Framework project was not identified. No formal Project Board meetings were held for the project.  **Risk**  The Commissioner, S151 Officer and Chief Fire |   Officer do not have clear oversight of key organisational / operational issues that both provides positive assurance that controls operate effectively and proactively identifies any areas of weakness. The project information and outcomes are not robust and cannot be relied on to support effective costs and benefits to the service. | In accordance with the Project Management Framework, the level of the project should be identified at the outset of each project.  A project board should be appointed for all level 1 projects to monitor the costs and benefits of the project to the service. | All AM’s and equivalents and GM’s and equivalents to be contacted to reinforce the following points –   1. Requirement to refer to the Project Management Framework when considering any new piece of work to identify whether workstream should be progressed as a project to support successful delivery. 2. Reinforce the need for all identified projects to clearly articulate the project level (level 1 or level 2). (Support will be provided by the CRMP Manager to discuss project methodology, project documentation and to assist determining project level. 3. Project level to be included on the SIP to ensure a list of level 1 and level 2 projects are maintained. | **Important** | Transformation Manager.   1. **Completed 31/03/2023** 2. **Completed 31/03/2023** 3. **Completed 30/06/2025**   **Projects are now included in the reporting framework. Projects are reported and reviewed at the services Continuous Improvement Board and a record of projects are maintained.** | 31st May 2023 |  |

**Project Management – May 2023**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Issue** | **Recommendation** | **Management Comments** | **Priority** | **Officer Responsible** | **Timescale** | **Status** |
| **2** | |  | | --- | | **Weakness**  The document approval section of the Project Closure/Evaluation Report has not been completed.  **Risk**  The Commissioner, S151 Officer and Chief Fire Officer do not have clear oversight of key organisational / operational issues that both provides positive assurance that controls operate effectively and proactively identifies any areas of weakness. The project information and outcomes are not robust and cannot be relied on to support effective costs and benefits to the service. | | In accordance with the Project Management Framework, the Project Closure/Evaluation report should be approved by the Project Executive for each project developed. | All AM’s and GM’s to be contacted to reinforce the following points –   1. Project SRO to ensure compliance with Project Management Framework for appropriate project closure and evaluation. (inc. follow up documentation capturing evaluation and outcomes) 2. SRO to review CBTF project and review closure and evaluation | **Important** | Transformation Manager   1. **Completed 31/11/2024 Projects are now incorporated into processes. Closure reports are completed and evaluation is measured against HMICFRS inspection pillars.** 2. **Completed 31/11/2024** | 31st May 2023 |  |

**2023/24**

**Risk Management Internal Audit – January 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **1 (c)** | **Risk and Impact**  Risk registers are not complete and risk actions are not appropriately tracked leading to the failure to effectively manage and address risks facing the organisation | Risk registers should be reviewed on a quarterly basis, ensuring that all sections of risk registers are fully completed, including controls and/or action plans to reduce risk to an acceptable score and reasoning for risk scores | **Medium** | Review of A30 Assurance and Performance policy by 31 March 2024.  **01/07/2025** A30 has been reviewed since this original recommendation. However, as the organisation continues to evolve, a further review is now required which will be undertaken later this year following the approval of a new corporate planning framework which will incorporate some elements of A30. | Assurance Manager  31st Mar 2024  New date.  31st Oct 25 |  |

**Risk Management Internal Audit – January 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **1 (d)** | **Risk and Impact**  Risk registers are not complete and risk actions are not appropriately tracked leading to the failure to effectively manage and address risks facing the organisation | Risk registers should be reviewed on a quarterly basis, ensuring that all sections of risk registers are fully completed, including controls and/or action plans to reduce risk to an acceptable score and reasoning for risk scores | **Medium** | Review SAB & QAR ToR to include quarterly risk review by 31 March 2024.  **Completed 3.6.24** This has been reviewed. Reporting of new and upgraded risks will be reported at PAP and Corporate Risk will be agreed and reviewed at SLT. | Assurance Manager  30th Sept 2024 |  |

**Risk Management Internal Audit – January 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **2(b)** | **Risk and Impact**  Insufficient training is provided on the risk management system leading to risks being inappropriately identified and recorded and the NCFRA not achieving best value for money from the use of the 4Risk system. | The training required for the 4Risk system should be determined and a structured training programme should be implemented for staff who use the system, with the training programme monitored for completion. This training should also include training on the principles of risk management in general.  A training plan / matrix should be developed for different levels of staff, which identifies exactly what level of risk management training is required for different levels or roles of staff. | **Medium** | Continuous Professional Training to be written and delivery by 30 June 2024 included in the management training programme to Middle and senior managers on the principles of risk management.  **01/07/2025** Claire chambers and Lisa Jackson have met to discuss a possible different approach to risk management. This is now being further explored with options being identified. | Assurance Manager  30th June 2024  New date 30th Sept 25 |  |

**Risk Management Internal Audit – January 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **3 (b)** | Risk and Impact: Risk management policies and procedures are outdated and do not reflect the organisation’s current working practices leading to risks being managed ineffectively. | The Risk Management Policy should be reviewed and updated, and the document control section updated to note the date of review and of the next review. | **Low** | Review all risk registers, once the risk policy and procedures are published for compliance, by 31 May 2024.  **Completed 01/07/2025** Departmental risk is reviewed by departments, with escalations reported to PAP. Corporate Risk is delivered through SLT meetings. A review of risk delivery is currently underway and any change will be factored into new process arrangements. | Assurance Manager  31st May 24  New due date  01/07/2025 |  |

**Grievance Internal Audit – March 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **1** | NCFRA have made a variety of changes to address causes for concern, areas for improvement and recommendations raised from HMICFRS reviews and the internal Serving with Pride consultation.  Whilst we confirmed there are HR KPIs in place to monitor grievance cases, and there is adequate reporting of progress made to implement recommendations, we noted there currently aren't any metrics to capture and quantify the impact of wider actions and changes.  We acknowledge that the Service are in the initial stages of implementing a number of recommendations, including those raised within Serving with Pride, however it is important to consider assurance mechanisms in the future to ensure recommendations are having the intended impact.  For example, the Service could use staff surveys to measure cultural changes such as the confidence in grievance processes. They could also use data from third parties to report the number of concerns raised via FRS Speak Up or Flag It, and then the number of grievance referrals subsequently made from this.  **Risk and Impact**: Changes and improvements made do not address HMICFRS causes for concern and NCFRA Serving with Pride recommendations. | Performance measures to substantiate and monitor the impact of changes made across the Service should be introduced to address HMICFRS reviews and NCFRA Serving with Pride recommendations. | **Low** | Accepted - The recommendations that have been highlighted within this audit are reasonable and are an area of focus for the Service to ensure that the impact of the various action plans is achieved. We will look at the different performance measures that are needed, including follow up staff surveys and measurement of the volume of speak up routes. An action date has been set in the future to allow time for implementation and impact of actions required to provide for meaningful feedback.  **Completed 01/07/2025**   * Grievance routes and learnings are collated and addressed in the BIO ER quarterly meetings to assess volume, trends, outcomes and where there are organisational learnings. | Suzanne McMinn  1st April 2025 |  |

**Payroll Internal Audit – April 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **4** | **Out of date Pay and Allowance Policy and inconsistent review cycle within Pay Policy.** NCFRA has several policy documents in place relevant to the payroll function and financial activities. Whilst our review of policies noted no concern over their appropriateness, we did note the following:   * Pay and Allowances Policy to be out of date and due for review since February 2022. * The Pay Policy March 2023 has a next review due date of March 2026,   however the Policy states that it is to be reviewed on an annual basis in consultation with the relevant trade union representatives.  **Risk and Impact:** NCFRA utilise out of date policies and has incorrect review cycles in place, leading to inconsistent approaches taken to financial and payroll activities. | * NCFRA should ensure that the Pay and Allowances Policy is reviewed on a timely basis, in line with its review cycle. * NCFRA should correct the review cycle inconsistency identified within the Pay Policy to ensure alignment with required Policy review cycle. | **Low** | Pay and Allowance Policy has not been updated, in line with their review cycle, by NCFRA. Incorrect next review due date in the Pay Policy compared to its defined monitoring and review cycle.  **Completed** **12.12.24** Update. Policy (V8) published on SharePoint today. | Nick Alexander/Suzanne McMinn  Due date  31st July 2024  New due date  31st Dec 24 |  |

**Identity Access Management (Joint) – June 2024 (Limited compliance)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **1.** | **Lack of Periodic User Access Reviews** 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. | **Medium** | 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.  **May 25** – TKJ update I've requested that this is the next audit we complete. The Audit Manager and Auditor have started. They have carried out an initial Locker Audit just to get in the swing of things so Audit activity will be in full swing soon. By 30/06 the audit will be underway by then or be in the process of reporting back to SIRO. | Trina Kightley-Jones, Head  of Information Assurance  31st Dec 2025 |  |

**Identity Access Management (Joint) – June 2024 (Limited compliance)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **2.** | **Multifactor Authentication for Fire AD Accounts**  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. | **Medium** | 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.  **13.1.25** YH update. A request for this action to be extended to Jan 2025 has been approved. Digital Security Architect developing paper for approval. On track | Roy Cowper, Enterprise Architect  30th Sept 2024  New due date  31st Jan 2025 |  |

**Identity Access Management (Joint) – June 2024 (Limited compliance)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **4.** | **Password Management Tool Implementation**  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 that 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. | **Medium** | 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.  **7.11.24** YH update, On track –  Currently in the commercial process for signing by the commissioner. | Andrew Jones, Head of Transformation and Change  31 July 2025 |  |

**Identity Access Management (Joint) – June 2024 (Limited compliance)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **5.** | **Completion of Access Changes**  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. | **Medium** | 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.  **7.11.24** YH update, On track - The procurement for the tool is progressing well. The revised project stage gates remain accurate. | Dan Cooper, Head of Technical Support  01 July 2024  New due date 31st July 25 |  |

**IT Asset Legacy Management (Joint) – June 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **1** | **Automated scanning of hardware and software is not used to identify inaccuracies in the IT asset register**  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. | **Medium** | 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.  **7.11.25** YH Update - Request to move dates due to procurement accepted. New due date 31.03.25 | Dan Cooper, Head of Technical Support -  DDaT  31 Dec 2025  New due date 31st Mar 2025 |  |

**IT Asset Legacy Management (Joint) – June 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **5** | **A formal IT Asset Management policy/procedure document has not yet been implemented.**  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. | **Low** | 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.  **27.1.25** JO update. Awaiting consultation finish date from Policy admin. | Dan Cooper, Head of Technical Support -  DDaT  30th Jun 2024  New date 31st July 2025 |  |

**2024/25**

**Safeguarding – September 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **1** | **The Service does not have oversight of whether all staff have been subject to a DBS check.**  Section 2 of the Rehabilitation of Offenders Act 1974 allows fire and rescue services to perform a minimum of a standard DBS check for all representatives. The Service’s Disclosure and Barring Policy outlines that a minimum of a standard DBS check is required for all staff and volunteers. Operational employees, who through the course of incident responses or targeted prevention / protection activities, carry out work with vulnerable individuals require an Enhanced DBS check. Rechecks are required every three years. The HR Projects Advisor maintains the Active Master DBS spreadsheet to record DBS data for employees, including certificate issue date, expected re-check date and any disclosures or bars on an individual. We conducted data analysis on the Active Master DBS spreadsheet in order to confirm whether all employees possessed an in date DBS. We noted the following:   * For 156 employees no DBS data was listed, including 61 firefighter personnel. * Eight employees were recorded as having up to date DBS checks however, there was no record to indicate whether they had disclosures or bars. * Three employees were recorded as having DBS checks without a re-check being performed.   The HR Projects Advisor informed us that when the HR Data Hub Team inherited the responsibility for managing DBS checks from West Northamptonshire Council (WNC) in April 2024, WNC did not provide the team with DBS information for a number of employees. Due to this, the Service implemented two phases of DBS applications to obtain DBS checks for those employees for whom it did not possess DBS information. The HR Data Hub Team is currently in the process of phase 2 and expects to have received DBS information from WNC for the outstanding 156 employees by the end of July 2024.  **Risk and Impact:** The Service is unable to confirm whether all staff have received a DBS check, potentially leading to individuals with undisclosed issues working in roles they may not be suitable for. | The Service should ensure it prioritises the completion of DBS checks for the 61 firefighter personnel at the earliest opportunity.  Following this, the Service should obtain DBS checks for the remaining 95 employees. | **High** | Final checks with WNC for those outstanding DBS checks to ensure no records held, prior to undertaking new DBS checks, to take place at the beginning of September. Outstanding DBS checks to commence as soon as possible.  **Completed 01/07/2025** DBS checking is now completed within the Fire service, all renewals are logged and new starters are subject to the same processes.  PDRA’s are completed with all DBS where required to do so. | June Withey  31st Mar 25 |  |

**Safeguarding – September 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **5** | **Completion rates of safeguarding training are not adequately monitored.** The Service requires its employees to complete National Chief Fire Council (NFCC) safeguarding training. The level of training required is determined by the likelihood that an employee will come into contact with a vulnerable individual, based on their role. As per the Service’s Safeguarding Adults / Children and Young People Policies, NFCC level one training should be provided to all staff and volunteers who come into contact with vulnerable individuals. Supervisory managers across the Service should complete NFCC level two. Designated leads should complete NFCC level four. Staff are required to recomplete the training at a two year frequency. We sought to confirm how oversight is maintained of the number of employees who are compliant with the Service’s training requirements. We observed that completion rates for NFCC level one training are monitored for all employees by the Competency Framework Team through Red Kite (Personal Development System).  Despite this, we were informed by the Prevention Team Leader that Red Kite does not currently possess the functionality to create a central log of all employees who have completed the additional NFCC training modules (levels two and four). Completion of these modules is instead currently recorded in an individual’s personal development record, which is only visible to the Line Manager. The Prevention Team Leader informed us that the Service intends to build new modules into Red Kite to allow the additional NFCC modules to be recorded within an individual’s safeguarding competency profile. This should then allow the Service to monitor completion rates of the NFCC additional modules across the workforce.  **Risk and Impact:** Employees may not complete the appropriate level of safeguarding training pertinent to their role and may not have the necessary skills or knowledge to appropriately deal with safeguarding matters. | The Service should:  1. Prioritise building new modules into Red Kite which facilitate centralised tracking and monitoring of all NFCC training levels.  2. Consider establishing an interim process for centrally  recording and monitoring the completion of additional NFCC  training modules. For example, through obtaining employee  training records from Line Managers and recording employee completion rates within a spreadsheet.  3. Conduct regular audits to ensure that all employees have  completed the required level of training. | **Medium** | The competency framework for NFRS staff has now been agreed and can be mapped into RedKite to improve recording of competency and the alignment of specific training modules to different competency levels.  This will include those training modules provided internally, from NFCC and from the Local Safeguarding Boards for Adults and Children. These will be provided by the Safeguarding Leads within the Prevention team.  This work will be added to action plans for the Training Department and will be undertaken by the Competency Framework Manager and Competency Systems Coordinator.  **Closed 01/07/2025** New Moodle platform is now live and training is monitored for completion. A new safeguarding package has also been created. | Neil Sadler  31st Dec 2024 |  |

**Safeguarding – September 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **6** | **Staff members are not appropriately chased to ensure mandatory safeguarding training is completed in a timely manner.** The Service requires all staff and volunteers who come into contact with vulnerable people to complete the NFCC level one safeguarding training module which is accessible via the Moodle portal. Staff are required to retake the module at a two year frequency. Completion rates for the module are monitored by the Competency Framework Team through Red Kite (Personal Development System). A reminder email is generated automatically based on the training renewal date. We reviewed an extract of the completion rates and noted that 95% of staff had completed the training. Three staff were overdue to retake the training and 24 staff were yet to complete the training. We selected a sample of two staff members who were overdue to retake the training and three who had not completed the training and requested evidence to support that they had been appropriately reminded by the Competency Framework Team. We noted the following:   * Two staff members were notified that the training was overdue one day after the two-year period ended (24/06/2024). However, after the initial notification no further reminder emails / escalations were conducted. The training was overdue by 41 days at the time of audit. * The three staff members who are yet to complete the training have not received any reminder emails / escalations. Each of them joined the Service between the 24/06/2024 and 15/07/2024. The current process is to set the training renewal date at two years from the employee’s start date. As such, these employees would not receive a reminder email until 2026 despite having never completed the training.   We were informed by the Competency Systems Co-ordinator that a robust process is not in place to continually chase individuals because following the initial automated Red Kite notification, any further correspondence has to be initiated manually. Due to  the number of training modules staff have to complete across the Service, it is considered unachievable to continually chase individuals manually. The Competency Systems Co-ordinator was in the process of finalising a proposal paper at the time of audit to manually update the renewal dates for mandatory training so that when new staff are enrolled, the renewal date is set for between one to three months of the employee’s start date. This is to ensure that the employee receives the  first chaser notification at a much sooner date.  **Risk and Impact:** Staff may not complete the mandatory NFCC level one safeguarding training on time and as such are not adequately prepared to handle situations involving vulnerable individuals. This increases the risk of harm or neglect. | The Service should:  1. Investigate whether the Red Kite system could be enhanced to automate follow-up reminder emails at regular intervals until the training is completed.  2. Adjust the process so that the training renewal date is set within the first few months of employment for new starters. This is to ensure that where training is incomplete, employees receive the reminder email within the first few months of employment instead of the current two year frequency.  3. Implement an escalation process where if a staff member does not complete the training after a certain number of reminders, Line Managers are notified and disciplinary procedures are carried out following repeat non-compliance. | **Medium** | This work will cut across Training and Workforce Development and so will be allocated to the two teams to work together. This will ensure that processes  for induction training, initial and renewed competency sign off are working effectively.  **Closed 01/07/2025** New Moodle platform is now live and training is monitored for completion. A new safeguarding package has also been created. | Neil Sadler  31st Dec 2024  New due date  31st Jan 2025 |  |

**Safeguarding – September 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **7** | **Performance reporting on DBS checks does not provide the SLT with adequate oversight.** The HR Projects Advisor uses the Active Master DBS spreadsheet to calculate DBS performance information, which is reported to the Senior Leadership Team (SLT) at a monthly frequency within the Fire DBS Check Update report.  We reviewed the three most recent Fire DBS Check Update reports (21/05/2024, 19/06/2024, 17/07/2024) in order to confirm whether each possessed an appropriate level of detail to allow the SLT to effectively monitor DBS Performance. We noted that each report did not include performance metrics outlining process times for DBS requests as well as tracking of DBS requests that are nearing / have reached the end of the three-year period.  In order to effectively monitor DBS performance, it would be beneficial for the Fire DBS Check Update report to include these performance indicators. This would provide the SLT with a more complete picture of the DBS process and allow them to make more informed decisions.  **Risk and Impact:** Incomplete performance reporting may lead to potential blind spots in the SLT’s understanding of the DBS process, negatively impacting decision making and risk management. | The Service should ensure that there is regular reporting of performance indicators that cover processing times for DBS requests and provide an overview of DBS’s close to / requiring a re-check such as the following:   * Average time taken to process a DBS check. * Number / % of DBS checks that require a re-check in less than a month. * Number / % of DBS checks requiring a re-check. | **Low** | Regular reporting of DBS checks by HR can be added to the Safeguarding Management Group agenda, this group has oversight of Safeguarding within  NFRS and has cross departmental representation.  **20.11.24** update. On trackfor completion by end of Dec 2024  **24.1.25** LB update - metrics have been agreed with HR colleagues and we received our first reporting into SMG. This will continue as BAU. | Lisa Bryan  31st Dec 2024  Completed |  |

**Asset Management (Joint) – October 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **1** | **Lack of Equipment Inventory Checks.**  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. | **Medium** | 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.  **28/06/2025** LH update – In progress and on track. | Leanne Hanson  30th Nov 2025 |  |

**Asset Management (Joint) – October 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **2** | **Lack of updated policies and procedures.**  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. | **Low** | 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.  **28/06/2025**LH update – In progress and on track. | Leanne Hanson  30th Sept 2025 |  |

**Asset Management (Joint) – October 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **3** | **Force – Lack of Equipment Testing.**   |  | | --- | | 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. | **Low** | **Police only action**  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.  **28/06/2025** LH update – In progress and on track. | Leanne Hanson  31st Nov 2025 |  |

**Asset Management (Joint) – October 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **4** | **Service – Reliance on spreadsheet for the Vehicle Maintenance and Records.** We noted that Fire Engines (pumps) are serviced every three months, six months and annually. While the Force uses TranMan to track maintenance and availability, the Service currently tracks this using a manual workbook tracked and updated by the Senior Fleet Administrator.  We noted that the TranMan Management system is available for NCFRA, but it is not utilised therefore, currently there is no availability tracking system used for fire trucks. Head of Transport and Travel aims to implement the use of TranMan for fire, we noted that this may be a potential area for training.  Additionally, we reviewed the sample of recently purchased fire fleet and noted that fire engine services were completed late for three out of eight vehicles. We noted that once the services were completed, they were dated and signed by the brigade technician and the supervising officer.  **Risk and Impact:** The use of spreadsheets, leads to human error as well as extra workload for operational staff. | Once the Service has transitioned to TranMan system, they should implement a programme of training on how to utilise the TranMan system for operational asset management staff. | **Low** | The Department is currently undergoing a review and potential restructure. As part of this work the maintenance of the Fire Appliances is being outsourced. Linked to this will then be a full review of all Policies and Procedures to take into account the revised delivery model. And then ensure that the incumbent system is utilised to its full potential whilst work is undertaken to implement a new fleet/equipment management system.  **28/06/2025** LH update – In progress. | Leanne Hanson  25th July 2025 |  |

**Core Financials (Joint) – November 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **1** | **Debtor invoices**  After the provision of goods or services to a customer or raising charges for services a request to raise an invoice should be sent to Finance Operations, who then complete an invoice template in order to automatically generate an invoice which is then sent to the customer by Finance Operations in order for the Force to receive payment.  We reviewed a sample of ten Force debtor invoices & found:   * Two instances where no request to raise the invoice could be evidenced. The invoices had been paid at the time of the audit. * One instance where the invoice had not been raised in a timely manner (29 days).   We reviewed a sample of ten NCFRA debtor invoices & found:   * Four instances where the invoice had not been raised in a timely manner (range of nine – 51 days and average of 36 days).   We were advised by management that there remains no formal timeline in place for raising of an invoice following a request.  **Risk and Impact**: Invoices are raised inaccurately or inappropriately leading to the Force not receiving income in a timely manner. | 1. 1. The Force should ensure that invoice request forms or similar are completed and provided to Finance Operations prior to the raising of an invoice and that this can be evidenced when required. Finance Operations should not raise an invoice until a valid request is received.   2. The Force and NCFRA should implement a clearly  defined timeline for the raising of invoices following a request being received to ensure invoices are raised in a timely manner. | **Medium** | Sales invoices will be centralised within the finance operations team. All requests will be raised via a service request and actioned. The turnaround time will be set at 3 working days, and the requestor will be automatically notified once the invoice has been raised. The go live for this will be 1st December  2024, with all parties in the organisation being made aware of the change, and how to raise sales invoices going forward.  19.1.24 NF update (Via RB)  Action completed | Annie Blake Finance operations team leader  1st Dec 2024  Completed |  |

**Core Financials (Joint) – November 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **2** | **Debt Recovery**  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. | 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 | **Medium** | 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 & 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.  19.1.24 NF update (Via RB)  Action completed | Annie Blake – Finance Operations Team  Leader, Nat Freeman – Head of Finance  1st Jan 2025  Completed |  |

**Core Financials (Joint) – November 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **3** | **New debtor set-ups**  In order for a new debtor to set up on Unit4 the debtor is to complete a new customer form and send it to the Finance Advice Bureau (FAB) Team at Northamptonshire who will then check the details and input them into the system. Once inputted it is expected that a different member of the FAB Team will approve the new debtor within Unit4 in order for the customer to become live and accessible.  We reviewed a sample of ten new debtors to the Force and NCFRA and, whilst we noted no issues with the Force samples, we did note one instance at NCFRA where  the same person had inputted and approved the same new debtor. We were advised by management that this error occurred due to a lack of training of a new member of the FAB Team and that there are no systemic controls in place within Unit4 that prevent a FAB Team member from approving a new debtor that they had originally inputted into Unit4.  **Risk and Impact**: There is a lack of systemic segregation of duty within Unit4 leading to new debtors being set up inappropriately. | NCFRA should ensure new members of staff are trained and fully aware of the segregation of duty requirements  between inputting and approving new debtors prior to gaining live system access.  2. The Force and NCFRA should work with Unit4 to implement systemic controls that prevent the workflow from allowing the inputter and approver to be the same person for new debtors. | **Low** | A new debtor set up will now be actioned within the finance operations team.  A new customer request form will be sent into finance operations. This will be checked to ensure that they do not already exist, and then set up as appropriate. Cross training has been carried out to ensure segregation of duties between the inputter and the approver.  This will also ensure that all information is requested and maintained from the outset to ensure debts are collectable.  19.1.24 NF update (Via RB)  Action completed | Annie Blake – Finance Operations team leader  1st Dec 2024  Completed |  |

**Core Financials (Joint) – November 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **4** | **Approval Limits of Write Offs in Aged Debt Process Document**  Included within the Force and NCFRA Aged Debt Process document is the steps and actions required before a write off can be approved and actioned and the delegated  limits for approvals. This includes write offs for salary overpayments above £500 which are to be sent to the OPFCC CFO for final approval of debt write off.  We reviewed a sample of ten write offs at the Force and noted two instances, both of which were salary overpayments valued at £1228.25 and £3275.81 respectively, where no documented evidence of OPFCC CFO approval could be provided for the write offs.  Management advised that the Force CFO is able to approve individual salary overpayment write offs up to £10,000 and whilst we confirmed, by review of email approvals, that the Force CFO had approved the write offs the Aged Debt Process document remains inconsistent with operational practices at the Force.  **Risk and Impact**: Inconsistent approaches taken to approval of salary overpayment write offs leading to recoverable debt being written off inappropriately. | The Force and NCFRA should update the Aged Debt Process document and ensure the delegated limits for writing off salary overpayments is aligned to operational  practices. | **Low** | Aged debt process has been updated to reflect the policies in place. The aged debt policy has an alert to ensure that it is not outdated. Regular write off meetings are held and documented.  19.1.24 NF update (Via RB)  Action completed | Annie Blake – Finance Operations Team Leader, Nat Freeman – Head of Finance & Nick Alexander – Chief Finance Officer  1st Dec 2024  Completed |  |

**Core Financials (Joint) – November 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **5** | **Credit Notes**  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. | **Low** | 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.  19.1.24 NF update (Via RB)  Action completed | Annie Blake -  Finance Operations Team  1st Mar 2025  Completed |  |

**Payroll – February 2025**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **1** | Expenses are submitted by members of staff within the Employee claim system.  Claims are self-authorised and there is no prior approval obtained when submitting a claim. The policy asks staff to speak to their line manager before seeking reimbursement and receipts should be submitted to support claims.  We selected a sample of 21 claims submitted by fire staff between April 2024 to September 2024, to assess whether the expenses policy had been followed. We noted several issues:   * Payroll Number 23-1800369: This individual had a claim paid of £112.25 in June 2024. This included a toll fare of £108. However, there was no receipt to support this transaction. * Payroll Number 23-1800125: This individual had a meal claim paid of £5.25 in July 2024. This included a food meal purchase of £40 that was paid. We were advised by management that this could be a group purchase. However, information should be submitted within the claim reason box to give as much detail as possible, which was lacking. * Payroll Number 23-1801002: This individual had a meal claim paid of £133.87 in July 2024. However, all the receipts provided were dated from March 2024. Therefore, this claim went back more than 3 months in contrast to the policy * Payroll Number 23-1800223: This individual had a meal claim paid of £58.05 in September 2024. The claim was in regard to four meals, but receipts of only three were provided. * Payroll Number 23-1800296: This individual had a meal claim paid of £118.24 in September 2024. However, it was difficult to reconcile the various receipts provided to the claim request. Management advised that with this individual it is difficult to match without a complete explanation from the claimant. | The Service should clearly communicate expectations regarding expenses to members of staff.  The Service should conduct regular spot checks of expense claims, with reconciliations of receipts and claims. | **Medium** | Agreed, we have set up a process to audit and check a proportion of the submitted expense claims for both accuracy and compliance on a regular basis throughout the year.  We have reviewed the claims with a senior fire fighter, and we are content that those claims are appropriate.  Michael Montgomery is issuing communications to make the expectations clear around evidence, accuracy and other compliance areas. | Nick Alexander Chief Finance Officer  30 June 2025 |  |

**Succession Planning and Promotions – June 2025**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **1** | We confirmed a risk assessment exercise had been undertaken in September 2023 to identify critical roles across the Service, and the impact if they left the Service. The critical roles are monitored at bi-monthly Workforce Planning Group meetings, however no formal succession plans have been put into place for the core or critical roles identified.  We take the view documented succession plans should be in place 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 Service is unable to fill key roles sufficiently quickly, leading to operational deficiency. | The Service should develop formal succession plans for critical roles to establish:  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;  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. | **Medium** | We acknowledge the audit’s observation that while some succession practices exist, a more structured and strategic approach to critical roles is required.  Critical roles have been identified, more work is required to develop the process and ensure that all competencies and qualifications are captured; and, job descriptions and specifications are under review.  The New PDR module (Talent Successor) has been implemented which provides the organizationally set development goals for those identified as part of a talent conversation to be cascaded and evidenced the system will hold details of staff that are identified within the talent progression pathways. The Platform also supports identification of staff and skill sets. All Talent pools are held on this platform enabling quick access to those who have been identified and their skill sets and/or aspirational skill sets.  Further work is required on this area, a workstream to review all the induction and handover processes will take place by the workforce development team. PDR & Effective 121 (inclusive of the importance of handover) has recently been designed and due to be rolled out in Autumn 2025 and form a part of the induction process for new line managers.  We are committed to maintaining a fair and transparent promotions process aligned with national guidance and best practice. The audit identified areas where communication and consistency could be improved to ensure fair and transparent promotion processes, we will:  Ensure that all promotion processes are underpinned by objective assessment methods and are clearly communicated to all staff.  Provide feedback to unsuccessful candidates to support their development.  Continue to monitor promotion outcomes to ensure fairness, equality, and representation across all demographics.  Improvements in these areas will be led by our Workforce Development department. | Mick Berry, Area Commander – Head of Response  01/10/2025 |  |
| **2** | We confirmed the Service has a clearly defined talent management process to identify, develop and support staff. For example, the D14 Talent Management and Progression Policy (May 2024) sets out the talent pool promotion process, as well as the High Potential Development Programme for high-potential staff and aspiring leaders.  Development objectives and talent conversations across the Service are subject to annual quality assurance sampling by the Workforce Development Team to ensure they are of adequate quality, depth and consistency. We also confirmed core learning pathways, talent matrices, and development objectives are used to develop staff.  We take the view that further action could be taken to communicate the measures in place to develop leadership and high-potential staff to ensure the process is open and transparent, in line with best practice across the sector. For example, the Service could:  Produce an easy guide of the talent pool promotion process and talent matrix, stored in an accessible location, so staff are sufficiently aware of the process and requirements.  Communicate the High Potential Development Programme to all staff, in particular staff with protected characteristics.  **Risk and Impact:** Staff are unaware of the processes in place to identify and develop high-potential staff and leaders, leading to missed opportunities to develop future leaders. | The Service should consider implementing the suggested actions to ensure the process for identifying and developing high-potential staff and leaders is adequately communicated and understood by staff across the Service. This will ensure the process is open and transparent for all staff. |  | **Completed 30/06/2025**  3transparent manner. In response to this, we have taken the following steps:  1. Leadership and Management Learning Platform: All staff now have full access to a comprehensive leadership and management learning platform hosted on Moodle. This platform provides a range of development resources and learning opportunities to support staff at all levels in building their leadership capabilities. All staff have access to a blended leadership programme at all levels inclusive of face-to-face learning, monthly learning resource mailout from WFD and access to the Moodle platform.  2. Updated Core Learning Pathways: Core learning pathways have been reviewed and updated to align with current organizational goals and leadership competency frameworks. These pathways are now published and easily accessible to all staff, ensuring transparency and consistency in development opportunities.  3. Policy Update: Policy D14, which governs leadership development, has been revised to reflect these enhancements and to further promote clarity and fairness in the identification and support of high-potential individuals.  These initiatives collectively support a more structured, transparent, and inclusive approach to leadership development across the organization. We will continue to monitor the effectiveness of these measures and seek feedback to ensure continuous improvement. | Jim Dorrill, Group Commander  30/06/2025 |  |