**INTERNAL AUDIT RECOMMENDATIONS DASHBOARD**

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

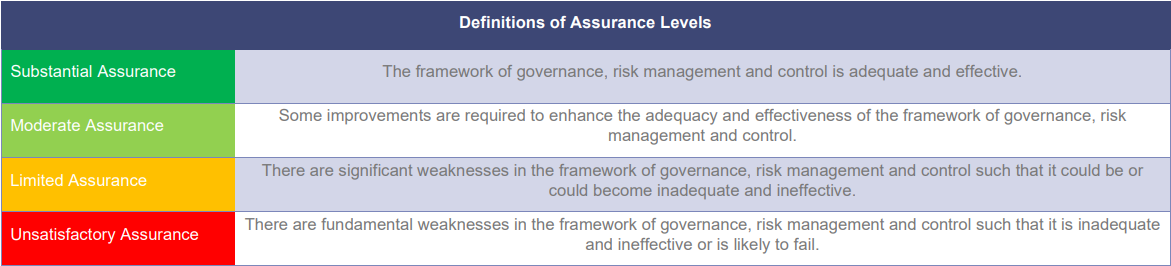
Audits are graded as Unsatisfactory Assurance, Limited Assurance, Moderate Assurance or Substantial Assurance.

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 |

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 |  | 2 |  |
| 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** | **2** | | |

| **2023/24 AUDITS** | **RECOMMENDATIONS MADE** | **High** | **Medium** | **Low** |
| --- | --- | --- | --- | --- |
| Risk management | 10 actions from 3 recs | 0 | 3 | 1 |
| Core Financials | 6 | Closed | | |
| Grievance | 1 | 0 | 0 | 1 |
| Payroll | 4 | 0 | Closed | 1 |
| 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** | **8** | **4** |

| **2024/25 AUDITS** | **RECOMMENDATIONS MADE** | **High** | **Medium** | **Low** |
| --- | --- | --- | --- | --- |
| Safeguarding | 7 | 1 | 4 | 1 |
| Asset Management (Joint) | 4 | 0 | 1 | 3 |
| **Totals** |  | **1** | **5** | **4** |

**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** | Programme Manager.  31st May 2023   1. **Completed**   31st May 2023   1. **Completed**   31st May 2023  **3. 23.11.23** MB update. Project framework reviewed, updated and published. Projects and project board need to be recorded and published. New due date 31.03.24  **3.6.24 –** LJ update**.** A review and evaluation has taken place around the project management framework and a paper has been produced a paper for SLT where Enabling Services and Business Services will work together and appoint from the outset Senior Responsible Officers, SME’s and all stakeholders to support project management and the change process into NFRS. The paper is being submitted to June SLT and expected completion if approved for Sept 2024.  **1.11.24** Awaiting update from Dan to confirm completion  **18/11/2024** D Retter update - Project process in place for all level 1 projects. The following still needs to be finalised:   * The assessment process that ascertains whether a project is  level 1 or 2. * Level 2 project methodology, including running and reporting.   This will be started in January 2025 – the CRPM has been prioritised and this bit of work has been pushed back. | 31st May 2023  New due date  31st Mar 2024  New date  30th Sept 2024  New due date 31st Mar 25 |  |

**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** | Programme Manager  **1. 23.11.23** MB update. Project framework reviewed, updated and published. Projects and project board need to be recorded and published. New due date 31.03.24  **3.6.24 –** LJ update. A review and evaluation has taken place around the project management framework and a paper has been produced a paper for SLT where Enabling Services and Business Services will work together. The framework will include all project stages including closure/evaluation. The paper is being submitted to June SLT and expected completion if approved for Sept 2024.  **1.11.24** Awaiting update from Dan to confirm completion.  **18/11/2024** D Retter update **-** SLT have approved the paper. The paper does not cover level 2 projects.  This will be started in January 2025 – the CRPM has been prioritised and this bit of work has been pushed back.  2. 3AM Operational Support. **Completed** | 31st May 2023  New date 31st Mar 2024  New date 30th Sept 2024  30th Sept 2023  New date 31st Mar 25 |  |

**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.  **3.6.24** LJ update – Assurance & Performance policy direction needs discussion with new Chief Fire Officer.  **31.10.24** RC update –A30 updated. Out for consultation in Nov. New forums will capture Internal Audit. | Assurance Manager  31st Mar 2024  Updated date 30th Sept 2024  New date.  31st Jan 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.  **3.6.24** LJ update –Both ToR’s can be reviewed once Assurance & Performance policy agreed with CFO.  **31.10.24** SAB & QAR ToR to be reviewed once A30 agreed.  New date 31st Jan 25 | Assurance Manager  31st Mar 2024  New date 30th Sept 2024  31st Jan 25 |  |

**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.  **3.6.24** – RC update. Delay due to HMICFRS inspection. New date 31.08.24 for everyone to complete.  **2.9.24** JO update – discussed with RC, need to consider a joint Police, Fire & OPFCC training requirement.  **31.10.24** RC update – Claire chambers and Lisa Jackson are to meet to discuss a possible different approach to risk management. | Assurance Manager  30th June 2024  New date  31st August 24  New date 30th April 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.  **29.5.24** JO update. Policy consultation feedback received. Procedures can now be written. New date 31st August 2024.  **2.9.24** JO update. Awaiting direction from A30 assurance & performance review & ToR’s for identification of where Risk is to be reviewed & monitored.**31.10.24** A30 drafted, awaiting ToR to confirm which forums will assure Risk to complete procedures. New date 31st Jan 25 | Assurance Manager  31st May 2024  New due date  31st Aug 2024  New date  31st October  31st Jan 25 |  |

**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.  **21.11.24** HR update. On track Being progressed through People & culture board. BIO meetings include track of grievances raised and lessons learned within the service. | Suzanne McMinn  1st April 2025 |  |

**Payroll Internal Audit – April 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **2** | **Expenses**. NCFRA’s Business Travel and Expenses Policy, last reviewed April 2021, states that expenses should be submitted through NCFRA’s employee claims system module on E-Works (NCFRA’s pay claims system), with receipts scanned and attached to the claim. Expenses claims are to then be approved by the individuals line manager on E-Works. We reviewed a sample of ten expense claims, between April and August 2023, and noted six instances where NCFRA were unable to provide any evidence to demonstrate the claim had been submitted on E-Works with supporting invoices and that approval had been obtained. The monetary range of these claims was £42.43 to £13.84 with an average of £25.09. Of the four expense claims where evidence could be provided from E-Works no issues were noted. Management advised that the current E-Works system is an old, unreliable, and failing system, which is at the end of its lifecycle for NCFRA, and is being replaced in April 2024.  **Risk and Impact:** NCFRA are unable to confirm that appropriate claims were submitted and approved for all expenses leading to expenses payments made by NCFRA not being for bona fide claims and amounts, resulting in financial loss to NCFRA. | * NCFRA should ensure line managers do not approve expenses unless a receipt is scanned onto E-Works and the completed claim is clearly identifiable and traceable. * NCFRA should investigate these six instances and establish why the claims are not present on E-Works. | **Medium** | Finance will issue communications to all Fire staff to remind them of their duties to include receipts. They will also complete dip sampling of claims to ensure appropriate receipts are included.  Finance will also review the 6 claims and contact the manager to see if receipts are available retrospectively.  **26.06.24** HR are reviewing the policy of March 2023 and following the migration to the new claims systems the wording of the policy is being proposed to be changed to ‘Expenses and Claim systems’ from specific systems and that any other amendments are considered. Suzanne McMinn & Nick Alexander will review this before passing for consultation.  **9.9.24** SMcM update – Policy out for consultation by mid Sept. New due date assuming 28 days consultation.  **30.10.24** Policy published. Completed | Nick Alexander  Due date 30th June 2024  Consultation & completion by 31st July 2024.  Completed |  |

**Payroll Internal Audit – April 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **3** | **Overtime.** NCFRA’s Raising a New Employee Claim procedural document presents how overtime claims should be submitted electronically through E-Works. As part of the electronic claim form, claimants are expected to complete personal details and add their claim details, such as claim reason for additional hours and the total number of hours and the rate, before submitting. The claimant’s line manager then reviews the submitted overtime claim and approves it on E-Works. We reviewed a sample of ten overtime claims, between April and August 2023, and noted five instances where NCFRA were unable to provide any evidence to demonstrate the claim had been submitted on E-Works with supporting evidence and that line manager approval had been obtained. Of the five overtime claims where evidence could be provided from E-Works no issues were noted. Management advised that the current E-Works –  is an old, unreliable, and failing system, which is at the end of its lifecycle for NCFRA, & is being replaced in April 2024.  **Risk and Impact:** NCFRA are unable to confirm that appropriate claims were submitted and approved for all overtime claims leading to overtime payments made by NCFRA not being for bona fide claims and resulting in financial loss to NCFRA. | * NCFRA should ensure that line managers do not approve overtime claims until required evidence and claims have been completed and uploaded onto E-Works. * NCFRA should investigate these five instances and establish why the claims are not present on E-Works. | **Medium** | NCFRA will issue comms to the organisation to ensure that managers are reminded of their responsibilities NCFRA are migrating to a new Duty Planning and overtime process, it is expected that this error relates to the issues with the existing system & these issues will be permanently resolved.  **NA Update** 22.10.24. Communications from the FSR implementation were sent on this and there were also workshops. The implementation of FSR has also now resolved the other issue re the identified claims.  6 monthly comms from the team are booked in to remind responsibilities.  Recommendation closed. | Rob Porter – System  Nick Alexander – Comms  Due date  30th Sept 2024  Completed |  |

**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.  **26.06.24**  As per earlier recommendation, the reviewed policy by SM & NA will be passed for consultation, by the required date to ensure that any old wording following migration is updated & any HR/ statutory updates are included.  **9.9.24** SMcM update – Policy being updated. New due date assuming 28 days consultation.  **13.9.24** CB update– Pay policy has been reviewed Jan 2024. HR to discuss with TU reps regarding need for annual review. Pay & Allowance policy review ongoing. New due date TBA by 20th Sept. Draft policy  **30.10.24** Policy out for 28 day consultation, new due date 31.12.24 | Nick Alexander/Suzanne McMinn  Due date  31st July 2024  New due date  31st Dec 24 |  |

**EDI – May 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **2** | **EQIAs have not been completed for all policies.** As noted in **Recommendation 2,** the NCFRA’s action tracker includes action EDI 3.1, which states “EDI Action Plan - All policies to be reviewed in light of revised EQIA approach". An EQIA is a critical tool in ensuring that an organisation’s policies are aligned to its strategic objectives in relation to equality, and in identifying instances where the impact of policies may be high in order to apply sufficient mitigations. We reviewed a list of all 112 current policies to ensure that an Equality Impact Assessment had been completed in all cases. From our review of the list, we note the following issues from the 112 policies included on the list:   * 60 policies had missed their review date (54%), with the largest "A27 -Responding to Town and Country Planning Applications" recording a review date of 22/11/2012. * 24 policies had not had an EQIA completed (21.4%).   We were advised by the Strategic Lead for Cultural Change that the fire service were aware of this, and a current process was underway to update all policies to ensure they are in date and have an EQIA.  **Risk and Impact:**  Policies are not compliant or consistent with the EDI strategy and general objectives of the organisation. Policies are out of date and do not reflect current practice, leading to an inappropriate approach that is inconsistent with the NCFRA’s objectives. | * As planned, NCFRA should continue as planned to carry out an EQIA for the remaining 24 outstanding policies. * NCFRA should update all policies that have missed their review date. | **Medium** | Policy updates are continually being reviewed. The EQIA process is part of that review.  **LJ update** – 22.10.24  EqIA’s are being monitored within the People and Culture Board & are being weaved into all projects, procedures, policies etc.  35 policies/EqIAs are out of date (29%). There are 2 policy/Plans that currently do not have an EqIAs. All of the owners have been reminded/chased. Closed | Lisa Jackson & Leo Holmes  Due date  30th Sept 2024  Completed |  |

**New systems Assurance – May 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **1** | **Detailed Payroll Procedures.** The NCFRA is moving away from an outsourced payroll function provided by West  Northamptonshire Council and is moving to an in-house payroll function sitting alongside the Force’s current payroll function with a planned go live date of 1 April 2024. The NCFRA will utilise iTrent as its new payroll system, which is the system already used by the Force, and due to this payroll staff are already aware of how to use the system. We undertook walkthroughs of system procedures and controls and found that there are currently not any NCFRA payroll procedures in place defining specific controls that will be in place and to provide guidance to staff processing the payroll, although due to using the same iTrent system as the Force most processes are expected to be similar.  For example, we were shown how the Unit4 HR system integrates with the iTrent payroll system with details of new starters added in Unit4 being transferred to iTrent,  however more detailed parts of the process were unclear such as whether there will be a checking and review process of the new starter details (e.g. bank details) added by payroll. At similar organisations we have found that procedural documents often include screenshots of the system supported by commentary to provide guidance to staff in completing day-to-day processes. This helps to ensure processes are completed consistently and also supports business continuity.  **Risk and Impact:** Without clear procedures and defined controls there may be a heightened risk of errors in payroll processing leading to incorrect payments to employees. | Detailed procedures and guidance should be developed for NCFRA payroll processes e.g. what secondary checks should  be undertaken by payroll when setting up new starters on iTrent, or the Force’s current procedures should be enhanced to cover the NCFRA as well. | **Medium** | Alongside the improvement work that is completed as a result of the Police Internal Payroll review, we are ensuring that all NCFRA and joint processes, and procedures and guides are being updated to ensure that they are effective for the future Business as Usual. As such, now that the NCFRA  implementation is complete and the dual system functionality scoping has been completed, we will ensure that all work across all payrolls (NCFRA, Police & OPFCC) is managed from joint processes and guides where possible to ensure uniformity and accuracy in processing and checking.  **26.06.24**System Payroll processes are being reviewed and refreshed processes will be internally made available to payroll (this is an internal payroll process only and guides on ‘how to’ for the payroll system will not be published externally to that team) team  Nick Alexander & Suzanne McMinn will discuss the Policies across pay to ensure appropriate updates.  **22.11.24** NA update - All processes have been reviewed; they are now available to all payroll staff within a centralised folder with one only being available. The have been diarised into the annual refresh plan and will be due for the annual review in the summer of 2025 | Nick Alexander & Suzanne McMinn (policies  only)  Due date  30 Sept 2024  Completed |  |

**New systems Assurance – May 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **2** | **Secondary Check of Expenses Claims.** According to the Fire Payroll Self Service Training Guide, employees should submit claims for expenses such as subsistence, mileage and spoilt meals via the MHR Payroll & Expenses Employee Self Service System (ESS). The Training Guide states that there is currently no line manager authorisation process for expenses, although audits will be conducted regularly. However, the Business Travel and Expenses Policy (March 2023) notes that in some circumstances such as when claiming for meals whilst travelling on business that employees should seek approval for the reimbursement prior to incurring the expenditure. Due to this the current policy relating to whether manager authorisation is required for expense claims is unclear.  **Risk and Impact:** Expenses claims are not reviewed or checked by payroll leading to payments being made to employees not in line with policy. | * Line manager approval should be obtained and documented when staff make claims for expenses via the ESS. * The Business Travel and Expenses Policy should be reviewed and clarification added as to whether line manager approval for expense claims is required or not. | **Medium** | As per the Police Payroll audit.  The risk of retrospective review is accepted and noted, however, the position remains the policy is that inappropriate claims will be managed through performance management 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.  **26.06.24** Michael Montgomery is reviewing guides in alignment to the Payroll audit recommendation to ensure they are effective for challenge and governance requirements, however, we will continue with the existing checks in place and the system will not move to further checks before payment.  **9.9.24 SMcM** update – Policy out for consultation by mid Sept. New due date assuming 28 days consultation  **30.10.24** Policy published. Completed | Michael Montgomery  Due date  30 Sept 2024  Completed |  |

**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.  **06/09/24**: PB update. 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.  **14.10.24** YH update  Consultation and recruitment underway, on track for completion by 31.12.2025.  **7.11.24** YH Update – on track. 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. | 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.  **06/09/24**: PB update MFA - Currently in 28 day consultation with Fire, Lisa Jackson to advise of consultation outcome.  **14.10.24** YH update. 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.  **7.11.24** YH update. New due date confirmed as 31.12.25 | 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** |
| **3.** | **Privileged Access**  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 time restricted 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. | **Medium** | 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.  **6.9.24** PB update. On track  **14.10.24** YH update.  Completed. PB confirmed completed in October JIAC. Privileged access management completed have seen the documentation this morning and so essentially achieved the timelines that were set out in the report. | Roy Cowper, Enterprise Architect  30th Sept 2024  Completed |  |

**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 Mar 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.  **6.9.24** PB update. Due to procurement activity and delayed ITSM implementation can these dates move to March 25?  **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 Mar 25 |  |

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **6.** | **Monitoring and Logging Policy**  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. | **Low** | 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.  **06/09/24**: PB update  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.  **YH update** – internal DDaT policy.  **PB update** within October JIAC monitoring & logging recommendation compete – have seen the documentation this morning and so essentially achieved the timelines that were set out in the report. | Roy Cowper, Enterprise Architect  30 Sept 2024  Completed |  |

**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.  **6.9.24** PB update. Due to procurement activity and delayed ITSM implementation request move to March 25.  **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** |
| **3** | **Assessments of IT infrastructure risks are performed on an ad-hoc basis**  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. | **Low** | 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.  **5.10.24** YH update - 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. Completed. | Roy Cowper, Enterprise Architect – DDaT  31 Dec 2024  Completed |  |

**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.  **06/09/24**: PB update  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.  **7.11.24** YH update - 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 consultation. New due date 31.12.25. | Dan Cooper, Head of Technical Support -  DDaT  30th Jun 2024  New due date  31st Dec 2024 |  |

**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.  **20.11.24** HR update –On track for completion by 31st March 2025 | June Withey  31st Mar 25 |  |

**Safeguarding – September 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **2** | **Irregularities in employee information between the ERP system and DBS monitoring spreadsheet.**  The HR Projects Advisor is responsible for maintaining the Active Master DBS spreadsheet (master spreadsheet), which is used to monitor the DBS status of the Service’s workforce. Upon receiving confirmation of an employee’s DBS, the master spreadsheet is updated to record the date of issue and expected re-check date.  The HR Projects Advisor receives weekly bulletins from the Service Information Team detailing starters and leavers. The bulletins are reconciled to the master spreadsheet to ensure that the master spreadsheet is up to date and includes all of the Service’s employees.  We conducted a reconciliation between a report of all employees extracted from Unit 4 (enterprise resource planning system) and the master spreadsheet using employee brigade numbers to determine whether the master spreadsheet included all of the Service’s employees at the time of audit. We noted that 20 employees were included on the Unit 4 report but not listed within the master spreadsheet. We queried these discrepancies with the HR Projects Advisor and were informed of the following:   * 14 were due to employee brigade numbers being incorrectly stated within the master spreadsheet. * One employee was initially a non-starter but later joined the Service which caused a delay in the HR Advisor being notified. * Two employees had been removed from the master spreadsheet as leavers however, had in fact only left their dual contract. * Three employees were external members of staff who did not require a DBS.   **Risk and Impact:** If the master spreadsheet is not kept up to date it will not accurately reflect the Service’s current workforce. Due to this, employees who require DBS checks may be missed leading to non-compliance with the Service’s procedures. | The Service should ensure that reconciliations are conducted between the master spreadsheet and an independent report of employees on a frequent basis (i.e. monthly) in order to identify data discrepancies and employees missing from the spreadsheet. | **Medium** | Mechanism implemented to ensure monthly checks of active employees against outstanding DBS checks. To commence with August end of month reporting and be embedded in the coming months.  **20.11.24** HR update – On track for completion by 1st Dec 2024. Report due to be pulled on this at the end of this month and will check it against those remaining on the DBS monitoring spreadsheet. | June Withey  1st Dec 2024 |  |

**Safeguarding – September 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **3** | **Inaccurate recording of DBS data.**  Service possesses a NFRS Employee For Checks spreadsheet which is used to monitor in progress DBS applications. Within the spreadsheet, HR Business Support Advisors record the date the DBS application was made and verified, as well as the result. Comments are added to outline any reasons for delays in processing the DBS, such as the employee failing to provide ID. Once the DBS check is complete, the issue date and certificate number is added to the NFRS Employee For Checks spreadsheet. The HR Projects Advisor then transfers the issue date and certificate number to the Active Master DBS spreadsheet, which is used to monitor DBS compliance across the entire workforce. We compared the most recent DBS disclosure received from WNC to the Active Master DBS spreadsheet for a sample of twenty employees, in order to determine whether the issue date, expected re-check date and content status2 had been accurately recorded within the spreadsheet.  We noted the following:   * One employee possessed no content as per the DBS disclosure email from WNC however, the employees content status was not recorded within the master spreadsheet. * One employees DBS was recorded within the master spreadsheet as having been issued 177 days after the actual issue date. This meant that the DBS would not appear to be due for recheck until 177 days later than required by the policy.   The HR Projects Advisor informed us that these discrepancies were due to errors made by staff members when manually updating DBS data. The Service’s current  process is to transfer data from the DBS disclosure email to two separate spreadsheets which poses an inherent risk of human error. The Service procured Unit 4 (Enterprise resource planning system) in April 2024 and plans to conduct a bulk upload of DBS data by August 2024. The Service anticipates that the use of this system will increase productivity by automating manual tasks and also reduce the risk of human error.  **Risk and Impact:** The Service’s current process is labour-intensive and prone to human error. This not only increases the risk of mistakes but also may lead to inefficiencies in HR operations. The recording of inaccurate data may lead to incorrect assumptions about an employee’s DBS status, potentially allowing individuals with unsuitable backgrounds to work in sensitive roles. | In the interim period before Unit 4 becomes live, the Service should:  1. Implement data validation checks to ensure that data has been accurately transferred from the DBS disclosure email to the spreadsheets. This could include conducting data analysis on the spreadsheets to identify missing or erroneous fields.  Spot checks could also be conducted on a sample of DBS checks each month to verify the accuracy of data transferred to the spreadsheets.  2. Consider whether the current process of transferring data to two separate spreadsheets is the most efficient and effective  approach, or if there are alternatives that could reduce the risk of error.  Following the implementation of Unit 4, the Service should ensure that the system is set up to automate tasks where possible to reduce manual input and includes robust data validation checks. | **Medium** | Access to GCON4 has been granted and expires at the end of October, so bulk uploads are to be completed before this date. This has been prioritised after the findings of this audit.  **20.11.24** HR update – This is completed. | June Withey  1st Nov 2024  Completed |  |

**Safeguarding – September 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Agreed Actions** | **Timescale/ Responsibility** | **Status** |
| **4** | **A robust process is not in place to ensure that DBS re-checks are conducted in a timely manner.**  We reviewed the DBS Policy in order to confirm whether it adequately outlined a process for ensuring DBS re-checks are conducted every three years in line with the Service’s policy requirement.  The policy includes high level stages such as that HR must inform the individual’s Line Manager when a re-check is required and escalate concerns to the Line Manager if the individual fails to comply. If an individual continues to refuse, HR’s disciplinary investigation route must then be followed.  Whilst a re-check process is in place, timescales have not been assigned to govern when each stage of the process should be conducted. For instance, the guidance does not specify the timeframe within which initial contact should be made with the Line Manager. Timeframes for when additional escalation steps should be initiated are also not stated. By setting clear deadlines, the Service can ensure that those involved in the process are aware of their responsibilities and when tasks should be completed. This can aid in preventing delays and maximising the probability that re-checks are conducted prior to the Service’s three-year deadline. This observation was supported by our sample testing, where we noted inconsistent  practices for three of our five re-check samples, which we have listed below:   * For three samples, initial contact was not made with the Line Manager until between 79 and 122 days after the end of the three-year period. * For two of these samples, an additional chaser email was sent 8 and 43 days after initial contact was made. A chaser email was not sent for the remaining sample.   Although the Service was not provided with the DBS data for these employees by WNC until after the end of the three-year period, the additional stages of the re-check process were applied inconsistently once notification was received.  **Risk and Impact:** Employees are not appropriately chased to ensure DBS re-checks occur in a timely manner. Due to this, the Service may not identify employees who are no longer suitable to work vulnerable individuals, placing those individuals at risk. | The Service should:  1. Establish clear timeframes for each stage of the DBS re-check  process, including when initial contact should be made, when reminders should be sent and when escalation steps should  be initiated.  2. Consider implementing an automated system that sends reminders when a DBS re-check is due following the  implementation of Unit 4. This could help in reducing delays and ensuring timely compliance.  3. Ensure that all individuals involved in the process are aware of their responsibilities and the importance of timely DBS rechecks. | **Medium** | Once Bulk uploads are completed as part of recommendation 3, we will be implementing the notification of expiring DBS Checks to the HR Transactional team.  **20.11.24** HR update - In place, notifications are set to go out prior to expiry date. Action can be closed once the next scheduled notifications due on 26th Nov are sent. | June Withey  31st Dec 2024 |  |

**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.  **18.11.24** NS update - The workstream is on track, work is ongoing with Training and Prevention to cross map the competencies | 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.  **18.11.24** NS update – The workstream is on track, work is ongoing with Training and Prevention to cross map the competencies | Neil Sadler  31st Dec 2024 |  |

**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 | Lisa Bryan  31st Dec 2024 |  |

**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.  **22.11.24** 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.  **22.11.24** 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.  **22.11.24** 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.  **22.11.24** LH update – In progress and on track. | Leanne Hanson  25th Feb 2025 |  |