**Agenda Item 7** **Report to the Joint Independent Audit Committee**

**02 October 2024**

**Internal Audit Recommendations Summary Report**

**RECOMMENDATION**

The Committee is asked to note this report.

1. **PURPOSE OF THE REPORT**
   1. This report provides the Joint Independent Audit Committee (JIAC) with an update on the status of actions arising from recommendations made in internal audit reports.
   2. The report contains actions arising from audits of Northamptonshire Police and the Office of Northamptonshire Police, Fire and Crime Commissioner and East Midlands Collaboration Units.
   3. The attached Summary of Internal Audit Recommendations Report shows details and the current status of all open audit actions.
   4. The Force Assurance Board has oversight of all outstanding audit actions and directs the activities required to complete any actions that have passed their targeted implementation date.
2. **NORTHAMPTONSHIRE AUDITS**
   1. **Overall Status**

The report shows in 2022/23, 2023/24 and 2024/25 a total of twenty-one audits have been completed, making seventy-six audit recommendations. Of those seventy-six recommendations:

* + - Sixty-one recommendations have been completed and are closed.
    - Three recommendations are recommended for closure.
    - Three recommendations have had their original implementation date revised and remain ongoing.
    - Nine recommendations have not yet reached their implementation date and remain ongoing.

Further details regarding mitigation activity and progress updates can be found within the attached report, Summary of Internal Audit Recommendations for JIAC September 2024.

1. **OVERVIEW**
   1. **2022/23 Audits**
      * Ten audits were completed making thirty-four recommendations all of which have been completed and are closed.
   2. **2023/24 Audits**
      * Ten audits were completed making forty-one recommendations.
      * Twenty-Seven recommendations have been completed and are closed.
      * Three recommendations are complete and are recommended for closure.
      * Eight recommendations have not yet reached their implementation date and remain ongoing.
      * Three recommendations have had their implementation date revised and remain ongoing.
   3. **2024/25 Audits**
      * One audit has been completed making one recommendation which has not yet reached its implementation date and is ongoing.
2. **COLLABORATION AUDITS**

* Two collaboration audits were completed in 2023/24.

**EQUALITY, DIVERSITY AND HUMAN RIGHTS IMPLICATIONS**

None

**HUMAN RESOURCES IMPLICATIONS**

None

**RISK MANAGEMENT IMPLICATIONS**

None.

**ENVIRONMENTAL IMPLICATIONS**

None

**Author:** Richard Baldwin,

Business Continuity and Risk Manager

**Chief Officer Portfolio Holder:** Paul Bullen, Assistant Chief Officer

**Background Papers:** Summary of Internal Audit Recommendations for JIAC September 2024.

2

**INTERNAL AUDIT RECOMMENDATIONS DASHBOARD**

**Summary of Audit Outcomes**

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

**Northants Audits 2022/23**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **AUDIT** | **DATE** | **GRADE** | **RECOMMENDATIONS MADE** | | |
| **Priority 1** | **Priority 2** | **Priority 3** |
| MINT Closedown Project | 17 May 2022 | Significant Assurance | 0 | 0 | 0 |
| Released Under Investigation Follow Up | 14 September 2022 | Limited Assurance | 1 | 0 | 2 |
| Complaints Management | 03 August 2022 | Significant Assurance | 0 | 1 | 0 |
| Balance Transfer | 03 March 2023 | Significant Assurance | 0 | 0 | 0 |
| Positive Action | 16 March 2023 | Significant Assurance | 0 | 1 | 0 |
| Reasonable Adjustments | 25 April 2023 | Limited Assurance | 2 | 3 | 2 |
| Data Quality | 02 May 2023 | Satisfactory Assurance | 0 | 2 | 1 |
| Risk Management | 03 May 2023 | Satisfactory Assurance | 0 | 5 | 2 |
| Information Management | 05 May 2023 | Satisfactory Assurance | 0 | 1 | 0 |
| IT Disaster Recovery | 09 May 2023 | Limited Assurance | 1 | 4 | 1 |
| MFSS Follow Up | 10 May 2023 | Significant Assurance | 0 | 0 | 0 |
| Medium Term Financial Planning | 10 May 2023 | Significant Assurance | 0 | 0 | 0 |
| Core Financials | 13 June 2023 | Satisfactory Assurance | 0 | 2 | 2 |

**2023/24**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **AUDIT** | **DATE** | **GRADE** | **RECOMMENDATIONS MADE** | | |
| **Priority 1** | **Priority 2** | **Priority 3** |
| Firearms Licensing | 21 July 2023 | Moderate Assurance | 0 | 2 | 0 |
| RUI Follow Up | 26 September 2023 | Moderate Assurance | 0 | 1 | 2 |

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

**2024/25**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **AUDIT** | **DATE** | **GRADE** | **RECOMMENDATIONS MADE** | | |
| **Priority 1** | **Priority 2** | **Priority 3** |
| Grant Funding |  | Substantial Opinion | 0 | 1 | 0 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Summary of Audit Recommendations Progress**

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **2022/23 AUDITS** | **RECOMMENDATIONS MADE** | **RED** | **AMBER** | **YELLOW** | **GREEN** |
| MINT Closedown | 1 | CLOSED | | | |
| Released Under Investigation Follow Up | 3 | CLOSED | | | |
| Complaints Management | 1 | CLOSED | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **2022/23 AUDITS** | **RECOMMENDATIONS MADE** | **RED** | **AMBER** | **YELLOW** | **GREEN** |
| Balance Transfer | 0 | CLOSED | | | |
| Positive Action | 1 | CLOSED | | | |
| Reasonable Adjustments | 7 | CLOSED | | | |
| Data Quality | 3 | CLOSED | | | |
| Risk Management | 7 | CLOSED | | | |
| Information Management | 1 | CLOSED | | | |
| IT Disaster Recovery | 6 | CLOSED | | | |
| MFSS Follow Up | 0 | CLOSED | | | |
| MTFP | 0 | CLOSED | | | |
| Core Financials | 4 | CLOSED | | | |
| **Totals** | **34** | **0** | **0** | **0** | **34** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **2023/24 AUDITS** | **RECOMMENDATIONS MADE** | **RED** | **AMBER** | **YELLOW** | **GREEN** |
| Firearms Licensing | 2 | CLOSED | | | |
| RUI Follow Up | 3 | 0 | 1 | 0 | 2 |
| Business Continuity & Emergency Planning | 5 | CLOSED | | | |
| Reasonable Adjustments Follow-Up | 5 | CLOSED | | | |
| Core Financials | 6 | 0 | 1 | 0 | 5 |
| Vetting | 3 | CLOSED | | | |
| Fleet Management Follow Up | 3 | CLOSED | | | |
| Payroll | 3 | 0 | 0 | 3 | 0 |
| Identity Access Management | 6 | 0 | 1 | 5 | 0 |
| IT Asset Legacy Management | 5 | 0 | 1 | 2 | 2 |
| **Totals** | **41** | **0** | **4** | **10** | **27** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **2024/25 AUDITS** | **RECOMMENDATIONS MADE** | **RED** | **AMBER** | **YELLOW** | **GREEN** |
| Grant Funding | 1 | 0 | 0 | 1 | 0 |
|  |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **2024/25 AUDITS** | **RECOMMENDATIONS MADE** | **RED** | **AMBER** | **YELLOW** | **GREEN** |
|  |  |  | | | |
| **Totals** | **1** | **0** | **0** | **1** | **0** |

**OUTSTANDING RECOMMENDATIONS**

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

**2022/23**

**Data Quality – May 2023**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| **4.1** | **Data Quality Training**  *Observation:* Data quality is integral to the integrity and validity of information used by the Force and OPFCC in both policing and non-policing operations. Therefore, it is important that all users who can create information are appropriately trained and have appropriate guidance to carry out this function. It has been noted that the training provided to users of specific systems (i.e., Unit4 and NICHE) includes limited inclusion for data quality and does not include any discussion regarding broader data quality issues or any of the impacts of inputting erroneous data.  There is also no general training on data quality provided to staff and/or officers to support the limited data quality training provided within specific system training. And, as has been noted below, there only seems to be guidance documentation in place regarding data quality for NICHE and not other systems, such as Unit4.  Additionally, within some systems it is possible to link records and previous audits across different Forces and systems have noted that this can lead to data quality issues if not appropriately trained.  *Risk*: Incorrect data entry or linkage can lead to errors in operations and damage to reputation and/or finances. | The Force and OPFCC should implement data quality modules as part of key systems training (i.e., NICHE and/or Unit4) that covers general data quality issues, common errors within these systems and the impacts of data entry and/or record linkage errors. | **2** | The recommendation is accepted.  Data quality training and education will be provided on a wider basis. In order to meet this requirement, a plan of activities will be drawn up, with responsibilities for delivery across the organisation  Assigned to Mark Manning  Update 19/03/2024:  Regional data quality report was received mid-February and will be discussed at FAB 16/04/2024.  Update 10/07/24 YH:  it is closed as the audit was specifically focused on Niche and Unit 4 and the requested data quality training has now been completed and captured within the DDaT Training plan. | Chief Digital Officer  December 2023  February 2024  July 2024 Complete |  |
| **4.2** | **Data Quality Benchmarking**  *Observation:* Benchmarking is an important tool for identifying areas of best practice and areas for improvement. Currently the Force engages with the Regional Data Quality team regarding data quality | The Force should ensure that information from the Regional Data Quality team is reported to the Information Assurance Board | **2** | Recommendation is accepted. | Chief Digital Officer  September 2023 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | issues within the regional NICHE system and from the national PND Data Quality Dashboard. However, this information is not reported back into the Information Assurance Board to be utilised in the identification of areas of focus and does not inform data quality strategies within the Force.  *Risk:* The Force is unaware how it's performing in data quality and cannot identify areas of best practice, areas for improvement or lessons learned. | and any issues are escalated as required to the FAB and/or JIAC.  Additionally, any issues, recommendations and/or learning presented should be reviewed by the Information Unit to determine how these can be rectified or implemented by the Force and/or OPFCC. |  | Information received from the Regional Data Quality team will be included in Information Assurance reporting to FAB.  Assigned to Sarah Crampton / Trina Kightley-Jones  Update 19/03/2024:  Report now received and submitted to FAB | February 2024 |  |
| **4.3** | **Quick Reference Guides**  *Observation:* Guidance documents provide quick and easy to understand information regarding individual topics. These are excellent formats for providing information regarding complex areas in small chunks, such as data quality for information recorded in NICHE. However, it has been noted that there is little information for other systems, such as Unit4, which could also be significantly impacted by erroneous data and/or poor data quality.  *Risk:* Incorrect data entry or linkage can lead to errors in operations and damage to reputation and/or finances. | The Force and OPFCC should create further guidance documents for each system in use to provide quick hints, tips and ""cheat sheets"" for ensuring data quality and integrity is maintained across all systems. This could include how to report data quality issues, how to record transactions in Unit4, etc. | **3** | Recommendation is accepted.  ‘Cheat Sheets’ will be produced as part of the first recommendation.  Assigned to Andrew Jones. Linked to Information and Data management risk – Niche ‘cheat sheets’ R0005.  Update 25/07/2024 AJ:  Action closed.   * there are user guides that have been in existence for some time and are regularly reviewed and updated. They are currently in the review process and can be found on the intranet here [Training Guides and FAQs](https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fnorthants.intranet.police.uk%2Fsystems%2Ffsp%2FPages%2Fguides.aspx&data=05%7C02%7CJackie.Bernard%40northants.police.uk%7Cd94dc7b706a34a5ce03808dcac73c1ab%7Cbf91f36fab8945038c3f04a029f837d3%7C0%7C0%7C638574860368826997%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=7HD2fm9nR8kMAOQJnnlIGXFvbMscfhKOyJW6N%2FzakVk%3D&reserved=0) [(intranet.police.uk)](https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fnorthants.intranet.police.uk%2Fsystems%2Ffsp%2FPages%2Fguides.aspx&data=05%7C02%7CJackie.Bernard%40northants.police.uk%7Cd94dc7b706a34a5ce03808dcac73c1ab%7Cbf91f36fab8945038c3f04a029f837d3%7C0%7C0%7C638574860368826997%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=7HD2fm9nR8kMAOQJnnlIGXFvbMscfhKOyJW6N%2FzakVk%3D&reserved=0) * there is very little end user input into the system with the majority performed by the relevant function ie Finance, HR etc. Those functions know the data format and errors will be due to not following process. To monitor data quality, separate data compliance checks are run frequently with feedback to the | Chief Digital Officer  December 2023  July 2024  July 2024 Complete |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  |  |  |  | functions owning the data to correct at source. |  |  |

**Information Management – May 2023**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| **4.1** | **Information Assets and Automated Decision Making**  *Observation*: While we completed our audit and found that controls were in place, adequately designed and effective, it was noted that we had only reviewed a sample of the systems in use at the Force and/or OPFCC; and, that there was little knowledge of automated decision-making processes within information assets, indicating a lack of maturity regarding information assets across the Force and/or OPFCC.  One particular issue was the lack of assessment of ADM within the current DPIA processes for new systems/activities within the Force and/or OPFCC. This was noted in the DPIA for the recruitment system which did not include information regarding the automated processing within the eligibility sift.  Additionally, Records of Processing Activities (ROPA) processes are used to detail the processing to be undertaken with personal data within systems and ADM is assessed using a single yes/no question and a free text box for comments. However, there is no requirement for this question to be answered and in cases reviewed, this reported back as “No Data”.  These documents are reviewed by the Information Unit and, if these questions are not required to be completed, they should be subject to greater scrutiny regarding this issue to ensure they are completed appropriately. Finally, it was also noted in both the Force’s and OPFCC’s privacy policies that an explicit assertion was made that no automated decision- | The Force and OPFCC should conduct a review of all existing information assets by asset owners, guided by the Information Unit, to ensure that all ADM processes are identified and assessed. Additionally, it should be ensured that DPIAs and ROPAs are reviewed to ensure that the relevant questions are appropriately recorded. Upon completion of the review the Force’s and OPFCC’s privacy policies should be updated in respect of automated decisions making. | **2** | Northamptonshire Police to refresh their Asset Owner Register and audit the current RoPA details to identify areas for update and to ascertain any other areas of Automated Decision Making  DPIA Templates to be updated to specifically identify automated processes particularly for new projects and business processes.  Review and refresh Privacy Notice and Policies  Update 13/05/24 – The RoPA and DPIAs are living documents so it is impossible to say that they are completely up to date. They are under review and it has become more reliable over time. The Records Manager is reaching out to business areas to get the most up to date position possible.  The restructure of Information Assurance will include new coordinator and support roles to work alongside the Records Manager and Information Assurance Auditor to check governance documents, including the RoPA, as part of pre and post audit activity and to ensure that governance documents and the RoPA are | Data Protection & Information Unit Manager  31/01/2024  Data Protection & Information Unit Manager 30/11/2023  Data Protection & Information Unit Manager 30/05/2024 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | making was undertaken on behalf of either organisation, which was clearly incorrect in respect of the recruitment platform. The phrasing also means it may be incorrect regarding automated decision- making undertaken by systems/platforms/processors outside of the Force’s/OPFCC’s knowledge.  *Risk*: Inappropriate processing of data using automated decision-making processes leading to regulatory action. |  |  | competed in respect of new projects. As RoPA becomes more reliable and stable it will enable cyclical annual reviews.  DPIAs have been updated and include a pre-DPIA checklist and specific reference to AI and automated decision Making and processing.  Privacy Notices still need to be reviewed and policies are currently being refreshed. Current demand means that a completion date for the Privacy Notices and Policy refresh cannot be estimated. The restructure of Info Ass is scheduled to be implemented by 01 September 2024 and this will release more resources for the more strategic activity.  13/08/2024  Paperwork in relation to data protection impact ass have been updated to include questioning around auto processes.  Assurance of the ROPA reflecting automated processes will be subject to annual review. Action complete. |  |  |

**IT Disaster Recovery – May 2023**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| **4.1** | **IT Disaster Recovery Procedures** *Observation:* There are no explicit procedures or runbooks relating to recovery in different disaster scenarios that may be required in the event DR is invoked. As Digital and Technology support both  police and fire IT applications that are hosted on-site and in Azure, it is likely that interfaces between applications may be disrupted causing the corruption of data.  Run-books should therefore define not just the technical steps to recovery such as reconfiguring the network and restoring data, but those steps necessary | Disaster recovery procedures should be developed that set out the overall recovery process, responsibilities and unique activities/considerations that may be required in the event of a disaster, such as resynchronisation of interfaces | **1** | DR procedures will be developed for core systems in Fire and Police, based on the BCP priorities  .   1. Agree which systems are ‘core’ 2. Gain business agreement 3. Create delivery plan for development of the procedures   Assigned to Dan Cooper  1. Agree which systems are ‘core’ | C Chambers, Chief Digital Officer  July 2023  September 2023  December 2023  March 2024 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | to re-establish the integrity of data and to recover services in an orderly way so as to optimise the speed of recovery.  We were informed that Force technicians can perform many recovery tasks such as restoration of data from backups; however, there are no procedures to cover those activities that only occur in a disaster.  *Risk*: The IT DR capability may not meet business requirements, which in a real disaster may lead to critical IT services either not being recovered on a timely basis or at all, thus causing significant impacts to Force operations. |  |  | 1. Gain business agreement 2. Create delivery plan for development of the procedures   Update from DC 19/03/2024:  Unable to complete this work due to other dependencies. All time lines associated with DR will now slip.   1. Agree which systems are ‘core’ 2. Gain business agreement 3. Create delivery plan for development of the procedures   Update from DC 02/05/2024:  DC is working alongside the Cloud Infrastructure Architect to establish and agree the Critical Systems. Meetings took place on 26/04 and 02/05 and the outcome of the meetings will be a defined list of Critical Systems.   1. Agree which systems are ‘core’ 2. Gain business agreement 3. Create delivery plan for development of the procedures   Update from DC 21/05/2024  Luke has built a DR matrix where we've categorised key business goals (like answering 999 calls, responding to incidents etc) into a plan of the rough order we would expect to recover infrastructure and systems in the event of a DR situation. As we work through each system we'll begin to get a feel for the level of criticality of each system and be able to put them into a category with a recovery point objective. Putting systems into the matrix will take some time, we have quite a lot!  Therefore could ask that the time line for the system analysis work is moved out until July and then the DR strategy to | April 2024  July 2024  September 2024  October 2024  January 2025  May 2024 TBC  TBC |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  |  |  |  | August please? This is a piece of work that Luke and I are actively working on so I don't see the need for any extension past that outside of maybe governance/approval cycles.  Update 11/07/2024 DC:   1. Agree which systems are ‘core’. 2. Gain business agreement 3. Create delivery plan for development of the procedures.   The matrix will be shown at the next CDO board on 17th July, which is hoped will provide guidance to next governance steps as well as giving a sitrep to progress so far.  Update 13/08/2024:  Finalised matrix and supporting documents stipulate overall recovery processes, responsibilities, activities and considerations. Action complete. | July 2024  July 2024  July 2024 |  |
| **4.5** | **Test Planning**  *Observation:* The Force do not have a standardised approach to testing. There is no overarching disaster recovery testing strategy in place and no tests have occurred beyond that done for the fire service relocation.  We were informed that there is some doubt that Oracle backups could be recovered within the RTO expected by the Force, but this concern has not been validated.  *Risk:* The lack of a defined testing strategy could lead inefficiencies in the recovery process which would in turn lead to inadequacies of the wider Force’s business requirements | A strategy for ITDR testing should be developed that reflects the operational challenges of testing DR arrangements while at the same time maintaining operational services.  Based on this an annual plan of disaster recovery tests should be maintained that that cover all services deemed critical to the Force. The plan should include services supported by failover arrangements as well as those recovered from backup.  Tests conducted should verify that services can be recovered |  | Strategy for ITDR will be written and taken to relevant governance groups for approval.  Assigned to Dan Cooper  Annual plan for testing will be drawn up, based on the audit recommendations.  Update 19/03/2024 (DC):  Unable to complete until the scope of systems is identified.  Update from DC 02/05/2024: | C Chambers, Chief Digital Officer December 2023  March 2024  C Chambers, March 2024  September 2024  TBC |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  |  | within the RTO expected by Force departments.  The development of disaster recovery procedures (see 4.1) should accommodate steps to test the failover of systems in an orderly manner so as to minimise disruption to the delivery of these services to Force employees |  | We are liaising with Gartner to produce an ITDR Strategy. Meeting taking place 08/05.  Update from DC 21/05/24 – As above for item 4.1  Update 01/07/2024 DC:  As above, the DR plan is on course for approval at the September 2024 CDO Board.  Update 13/08/2024:  Testing schedule for all critical systems now developed. Fire testing schedule now in place monthly to enact DER process (Warwickshire). Action complete. | August 2024  September 2024 |  |
| **4.6** | **Updates on the status of DR Arrangements** *Observation:* There are no formal updates to business continuity stakeholders such as the emergency planning team on the adequacy of disaster recovery arrangements.  *Risk:* The wider business are unaware of the Force’s disaster recovery arrangements and therefore whether these adequately meet their requirements | The Force should implement formal arrangements to ensure that that business continuity stakeholders such as the emergency planning team are updated upon the adequacy of IT resilience and disaster recovery arrangements. | **3** | The strategy detailed in the previous recommendation will include formal arrangements for reporting to key stakeholders, ideally via a governance group that is already in existence.  Assigned to Dan Cooper Update 11/07/2024 DC:  Once written and first draft approved (due September 2024) the plan can be scrutinised by any number of teams. The preferred direction is to have a plan first, then adapt to the any specific stakeholders rather than have those stakeholder meetings with a blank piece of paper.  Update 13/08/2024: | C Chambers, Chief Digital Officer  December 2023  December 2024 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  |  |  |  | This action has been completed via the completion and approval of the matrix and supporting documents and has been through all required governance and approval cycles. Action complete. |  |  |

**2023/24**

**Firearms Licensing – July 2023**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| **4.1** | **Delays in Decision Approval and Certificates** *Observation:* All grant and renewals applications are required to be appropriately approved, under Section 55 of the Firearms Act, by the Firearms Licensing Manager or Deputy Firearms Licensing Manager. This approval is evidenced in the Force's Enquiry Pack, with a step for the approval, printing and signing of each certificate issued.  Audit has reviewed 15 grant applications and 25 renewal application to confirm that appropriate approval has been provided and while this is clearly evidenced, it has been noted that there have been significant delays.  Of the 40 applications reviewed, 25 were approved more than 30 days after the Enquiry Pack was completed and submitted by the FEO; 11 were printed more than 5 days after being approved; 17 were printed prior to approval being provided; and 26 were 2signed more than 5 days after being printed.  Throughout our audit we have noted a significant backlog of cases within the Unit, which has been the major factor in preventing the timely processing of applications.  Whilst there are no statutory timeframes for the processing of firearms license applications, the current | The Force should analyse the firearms license process to identify specific actions to address the current backlog.  This should include a root cause analysis of the backlog and identify areas for optimisation. | **2** | A root and branch review has been carried out by a D/Supt who has been based in the unit, a report was presented to Chief Officers.  Peer Review carried out by other force FELU.  A demand analysis was also completed, the findings of which were taken into the above review paper.  Currently working on a paperless system to support a more efficient process as well as a review of staff roles and responsibilities.  Update Jan 24 - This is ongoing and work is underway to restructure some of the roles within FELU to make it more efficient. The process to Digitise the Unit is also progressing at pace and the NICHE module for this is now being tested, with it aiming to be implemented by March 2024/ Further work to single online home and automation  / robotics will see further significant performance improvements. | Head of Central Intelligence Services  Completed  Head of Central Intelligence Services Ongoing |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | level of delays impacts on application satisfaction and Force reputation.  *Risk:* Significant delays in the approval of firearms license applications increases the risk of new and changing circumstances not being included within the assessment. |  |  | A further review was completed internally which will serve to further improve processes within FELU.  Update May 2024  Grant backlog is now at 178 and decreasing (of those 50 are longer term contentious decisions, so sit outside the SLA meaning the outstanding backlog is 128 and falling). The renewals backlog is 316 (of those 103 are longer term contentious decisions, so sit outside the SLA meaning the outstanding backlog is 113 and falling).  NICHE digitisation process is also continuing and has become embedded, and staffing is good in the team. |  |  |
| **4.2** | **Delays in Contacting Applicants and Conducting Home Visits**  *Observation:* All grant and renewals applications are required to be subject to a home visit and security inspection carried out by a Firearms Enquiry Officer. This is evidenced in the Enquiry Pack through detailed notes taken by the FEO.  Audit has reviewed 15 grant applications and 25 renewal application to confirm that clear and appropriate evidence of these inspections has been provided, and while this is clearly evidenced, it has been noted that there have been delays.  The delay is occurring while waiting for the FEO to contact the applicant, with 31/40 cases not being contacted within 30 days of an FEO being appointed. The delay in visitation can cause unnecessary work if there is change of circumstance between application and visit as this may require updated or new application information to be recorded and assessed. *Risk*: Delays in conducting home visits may allow for changes in conditions to be unobserved by FEOs or for | The Force should allocate casework to FEO’s on a more timely basis.  The Force should communicate expected timeframes for actions to be taken. | **2** | Casework is allocated to FEOs, however, due to resourcing within FEO team, visits to holders are significantly delayed, resourcing is being reviewed as part of current scrutiny of unit. On line application (SOH) gives indication of timeframes/delays at present.  On FEO visit, holders are requested to sign a disclaimer stating there have been no changes in circumstances since they submitted the application, any changes are discussed and noted on enquiry pack. FEOs are not pressured to clear applications, emphasis is placed on thorough and robust enquiries.  Recent Mowbray review found that there are no shortcuts in relation to enquiries due to backlog that would increase risk to public safety. | Head of Central Intelligence Services  Continuous Review  Cannot be achieved until backlogs are removed. |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | | RUI 1-2 Years | RUI >2 Years |
| Apr 21 | 328 | | 139 |
| May 22 | 242 | | 113 |
| Jun 23 | 217 | | 86 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | FEOs to feel pressure to clear applications due to the length of time they have been being processed. |  |  | Update Jan 2024 - Visits to holders for new grants is progressing including using overtime with funding provided by the OFPCC. This will have a substantial impact on improving the time taken to deal with an initial grant. Further work realigning resources within the department will also reduce time taken.  Update May 2024  As above – timeliness has improved and is improving. |  |  |

**RUI Follow Up – September 2023**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| **4.1** | **Longstanding RUIs**  *Observation:* As per the previous review, it was identified that it was necessary to prevent longstanding RUIs due to the negative effects they may present to afflicted individuals, particularly for those in the course of undergoing employment or other vetting processes. Although there has been a reduction in the number of longstanding RUIs over time, a large number of individuals still remain RUI for over one year.  Below is a summary of the status of longstanding RUIs at the time of our audits:  The responsibility for the review of longstanding RUI cases lies with Chief Inspectors, and on a quarterly basis Chief Inspectors are requested to undertake a | The Force should explore how officer’s 28-day review of RUI cases can be monitored.  The Force should actively monitor and report on longstanding RUIs to ensure that accountability and ownership is in place for individual Chief Inspectors, such as by sending RUI figures reports to a board or committee for review. | **2** | The force accepts the recommendations. The force will consult on a standardised automation process to assist with monitoring of reviews to identify where further improvements can be made however, RUI’s have continued in a downward trend, and I am satisfied that the 28-day review process is sufficient to manage risk in the interim.  The Aged RUIs will be reviewed yearly as part of the Senior Officer Review process to drive down the numbers, and individual Chief Inspectors will be sent the data on a quarterly basis.  Governance will be via Improving Investigations Board.  Update from AR 07/08/24 - Longstanding RUI levels remain constant since 2022. | 6-9 months depending on technical requirement - DCI Andy Rogers |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | review of longstanding RUI cases, last taking place in May 2023.  The Detective Chief Inspector now holds a meeting every week with Custody to discuss RUI cases.  Additionally, RUI cases should be reviewed every 28 days by officers however this is a personal responsibility of officers and is not monitored.  We noted that the Force has the capability to actively monitor RUI figures through Niche reports that can be generated, however, these figures are not reported more widely.  *Risk*: Individuals on longstanding RUI are not treated fairly and may present a risk of reputational damage to the Force. |  |  | Recommendations:   * All RUI’s over 1year (315) to be reviewed, initial direction after report creation to come from OIC Supt’s to cascade and own. Then, when next feasible, long term RUI’s to be reviewed as part of the Senior Officer Review process. Officers who have failed to update/progress to be managed accordingly through the review process and line manager. * Within this recommendation I believe it to be necessary to add the review of Bail. I propose that I review all bail cases over 6months (23) to see if case remains applicable or is an admin issue. Once completed, review issues and patterns then progress to 3-6months. The necessity is that I have checked 3 cases, both need finalising with custody being updated for RUI/Bail closure and would be an easy data cleansing exercise. In addition, it would prevent legal action if we were showing an individual as under a live investigation when their case has been NFA’d. * A new report to be developed to capture total date from arrest and not just when RUI or Bail. This will provide full data on cases where a suspect has been processed as such, as at present you can have a Bail case between 3- 6months and if reverted to RUI it will then go into the 0-28day list. It does not show the full picture of where are cases are being progressed. * Custody Bail Sgt to review RUI with filed occurrences, in the short-term fix to sort this as the process should be managed by the OIC and their Sgt. |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  |  |  |  | Update 09/09/24 – All of the recommendations outlined above have been implemented and will be reviewed on a bi-monthly basis. Recommended for closure. |  |  |
| **4.2** | **RUI Concerns**  *Observation:* As per the recommendation from the September 2022 review, the Force is taking steps to ensure that RUI cases are reviewed.  Previously, the Detective Chief Inspector undertook a personal review of RUI cases, however, due to time constraints no longer personally reviews them. A RUI spreadsheet is forwarded to Chief Inspectors on a fortnightly basis to identify if RUI was the correct choice or if bail should have been considered.  Chief Inspectors then distribute the cases to their teams who note whether RUI was the correct choice and provide a rationale. If errors have been identified during the review process, the officer reports back to the Detective Chief Inspector with the rationale and these cases are saved into a folder.  From discussion with the Detective Chief Inspector, no repeat offenders have been identified so far. However, we did not find that standardised categories of errors are in use as per the previous recommendation.  *Risk:* Repeated errors in processing RUI’s are not identified and remedied. | The Force should develop standardised categories of error to assist in the identification of common errors and for use in future reporting, communications and training. | **3** | The force accepts the recommendations. The force will consult on a standardised automation process to assist with monitoring of reviews to identify where further improvements can be made however, RUI’s have continued in a downward trend, and I am satisfied that the 28-day review process is sufficient to manage risk in the interim.  The Aged RUIs will be reviewed yearly as part of the Senior Officer Review process to drive down the numbers, and individual Chief Inspectors will be sent the data on a quarterly basis.  Governance will be via Improving Investigations Board.  Update from AR 07/08/24 - Longstanding RUI levels remain constant since 2022.  Recommendations:   * All RUI’s over 1year (315) to be reviewed, initial direction after report creation to come from OIC Supt’s to cascade and own. Then, when next feasible, long term RUI’s to be reviewed as part of the Senior Officer Review process. Officers who have failed to update/progress to be managed accordingly through the review process and line manager. * Within this recommendation I believe it to be necessary to add the review of Bail. I propose that I review all bail | Initial phase to identify standardised categories 3 months, with ongoing monitoring for compliance - DCI Andy Rogers |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  |  |  |  | cases over 6months (23) to see if case remains applicable or is an admin issue. Once completed, review issues and patterns then progress to 3-6months. The necessity is that I have checked 3 cases, both need finalising with custody being updated for RUI/Bail closure and would be an easy data cleansing exercise. In addition, it would prevent legal action if we were showing an individual as under a live investigation when their case has been NFA’d.   * A new report to be developed to capture total date from arrest and not just when RUI or Bail. This will provide full data on cases where a suspect has been processed as such, as at present you can have a Bail case between 3- 6months and if reverted to RUI it will then go into the 0-28day list. It does not show the full picture of where are cases are being progressed. * Custody Bail Sgt to review RUI with filed occurrences, in the short-term fix to sort this as the process should be managed by the OIC and their Sgt.   Update 09/09/24 – All of the recommendations outlined above have been implemented and will be reviewed on a bi-monthly basis. |  |  |
| **4.3** | **Training**  Observation: Subsequent to the September 2022 review the Force have proactively sought to increase the completion rates of NCALT Bail and RUI training by officers.  However, changes to the Bail Act in October 2022 have made the previous training obsolete and new pre-charge bail training has been implemented, which | The Force should proactively pursue completion of pre-charge bail training. | **3** | The force accepts this recommendation. This will be part of the training and implementation plan introduced as part of the new Bail Reform Act 2022, being rolled out during October 2023 as stated.  Communications to drive improvements in | 4 months - DCI Rogers |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | will become mandatory from October 2023. Currently, a large number of officers have not yet completed the training:   * 138/1524 – pre-charge bail e-learning completion * 558/1524 – pre-charge bail video   Although it is not yet mandatory, audit believe that it would be best practice to continue proactively increasing the completion rate for training to mitigate the risk of bail and RUI being administered inappropriately.  Risk: Officers in the Force are inadequately trained and RUIs / bail are incorrectly processed. |  |  | completion rates of training prior to it being mandated will be pursued.  Update from AR 07/08/24 - I propose that the total figures for Bail training completion to be ran again and to confirm with training that this is now part of the student officer training supported previously.  Custody are the gatekeepers for bail, and I have not seen anything to concern me about bail. This is supported with very few concerns highlighted from previous reviews (pre December 2023) with RUI being used on high-risk cases where Bail could/should have been utilised.  Roll out RUI/Bail training for Sgt’s due to the change as part of their first line manager course. |  |  |

**Business Continuity & Emergency Planning – November 2023**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| **4.2** | **Contingency / Response Plans**  *Observation:* The Joint Operations Team (JOT) is responsible for the management of Contingency Plans for sites within Northamptonshire. A Testing & Exercise Calendar is maintained by JOT, which includes a schedule of planned exercises for 2023 for a number of different exercise categories, such as with the LRF, regionally and the Force.  The JOT also audits Contingency Plans and produces a spreadsheet noting when the Plan was last updated, with an audit last taking place in January 2023. We noted that there are approximately 246 in the ‘Response Plans’ category, and upon further review found: | The Force should review and update its outdated Contingency Plans as soon as possible and determine which Plans should be updated as a priority.  Additional resources should be allocated towards locating, reviewing and updating Contingency Plans. | **1** | The ability of the Joint Operations Team to review effectively the current contingency plans was highlighted in the June 2022 review that saw the recommendation for the uplift in the department of two full time PC’s. These have now been recruited and with a change of one other PC who obtained a new role there are now 3 new PC’s within JOT who are now undergoing the relevant training in event planning and contingency plan writing and reviewing.  A light touch review of plans was undertaken over the last year to ensure contact details and agencies were still | Staffing recruitment now complete.  Staffing training complete by January 2024.  Plan for allocation of plan reviews in line with risk now complete. |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | * 102/246 – last updated more than two years ago. * 31/246 – last updated between one year and two years ago. * 37/246 – the plan could not be found.   We also selected a sample of four Plans in order to confirm whether testing was undertaken recently. In two cases, we were informed that Plan specific exercises and testing have not been undertaken recently, although other exercises carried out covered some aspects of these Plans, such as the mobilisation of resources.  *Risk:* Emergency Response and Contingency Plans are outdated and / or not fit for purpose, leading to an ineffective response to emergencies. |  |  | relevant but no detailed analysis was undertaken due to Operational Demand and staffing levels.  A plan has now been enacted to fully review the current response plans in risk order compared with the National Security Risk Assessment and Northamptonshire Community Risk register.  This work will now be ongoing and reviewed every 6 weeks with all staff in the department being allocated individual plans for detailed review. 20 plans have been allocated in the first tranch. The Counter terrorism plans are reviewed on a quarterly rotating cycle led by CT EMSOU via the NAPRAS process.  A large number of the documents in the site specific are not owned by Northants Police but will need to be reviewed with the site or partner agency for relevance.  28/05/24 Update. After a detailed supervisory review of the Response Plans, Operational orders and Operational guidance on the JOT Homepage the 246 plans & documents that existed at the time of the audit in November 2023 have been reduced to 138. Of these over 40 have been reviewed or are currently under review. They have been prioritised based on the new Community Risk Register Group of risks and the CT guidance around the NAPRAS process and Crowded Places. | Review of all plans estimated timescale 2 years. (Oct 2026) |  |
| **4.3** | **Training and Guidance**  *Observation:* The Force’s Business Continuity Management Policy states that individual Business Continuity Plans (BCPs) will be developed for each department within the Force. Departmental managers are responsible for managing the BCPs for their respective departments.  We interviewed the BCP owners from four departments and found that they received no initial or | The Force and OPFCC should implement appropriate training programmes for responsible owners of BCPs upon initially becoming responsible, as well as continuously.  Awareness of business continuity guidance located on the Force’s | **2** | OPFCC – Accepted  Update 8th Jan 2024 – We will seek the support of the Force about awareness training and follow guidance as far as possible used by them as the larger organization. | 28th February 2024  Force Business Continuity and Risk Manager November 2023 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | continuous training related to BCPs. Whilst audit acknowledges that informal training is available on request and guidance is accessible on the Force’s intranet, interviews conducted by the Force highlight that not all responsible owners are aware of the support available to them.  From discussions held with the Director of Delivery, we noted that no formal training is in place around the OPFCC’s Business Continuity Plan (BCP). We were informed that staff members are made aware that there is a BCP and where it is located, however this has not been formalised such as in the induction process.  *Risk:* Responsible individuals do not have sufficient understanding and accountability of the business continuity processes. | intranet should be communicated to all responsible owners across the Force.  It should be ensured that the induction process for new staff members includes training and guidance relating to BCPs. |  | Force - Additional BC Awareness guidance and training will be developed to supplement the existing BCP Guidance.  This will be communicated to all staff through Force Orders and Forcenet with additional training offered to those that require it.  Update 20th Mar 24 – BC Guidance produced and published, and Policy and Procedures updated. |  |  |
| **4.5** | **Contingency Plans Procedures & Guidance** *Observation:* The Joint Operations Team (JOT) has developed a Contingency Plans Procedure. The Procedure notes that the Force response to major incidents is noted within the Multi-Agency Response Manual (MARM), which is maintained by the LRF and is located on Resilience Direct, and that JOT is responsible for contingency plans relating to Northamptonshire.  The Procedure states that there are two main types of plans, Specific Contingency Plans and Area Contingency Plans, and that the purpose of the Procedure is to provide a standard for the format of Area Contingency Plans which are required to follow a common pattern.  Upon review of the Procedure, we found that it only provides limited detail on the required format and structure of Area Contingency Plans, and a standard template for plans is not included within the Procedure. We also noted that the Procedure does not include information on how often plans should be reviewed, and how and when exercises and testing should be carried out.  We also found that the Procedure only provides limited information on roles and responsibilities of specific staff members. The JOT supervisor is noted as | The Contingency Plans Procedure should be reviewed annually, and should also be updated to include information such as:   * Contingency plan template (or link to a template). * Specific roles and responsibilities. * How often contingency plans should be reviewed and updated. * How and when exercises and testing of contingency plans should be carried out. * Communication protocols e.g., a list of key contacts.   Updated copies of guidance noted within the JOT audit spreadsheet should be obtained, or the guidance removed if no longer relevant. | **2** | The Contingency Plans Policy & Procedure and Operational Order Policy & Procedure ownership have now been transferred from Sergeant ownership within JOT to the Inspector for JOT and are now being reviewed.  They will contain:  A Contingency plan template (and a link to a template).  An Operational order plan template (and a link to a template)  Specific roles and responsibilities.  How often contingency plans and standing Operational Orders should be reviewed and updated.  There is now a seconded Police Sergeant based in JOT who is reviewing the testing and exercise program in co-ordination with the LRF partners. A TOR is now under discussion between the LRF partners. This will address how and when exercises and testing of contingency plans should be carried out both single agency (Police) and Multi Agency (with wider LRF partners). | Policy & Procedure reviews Completion anticipated by December 2023.  Testing and training Role and guidance: December 2023.  Review of relevant guidance documents on JOT homepage December 2023. |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | being responsible for signing off plans, however, responsibilities for the wider team and Force is not included.  Additionally, we noted that the Procedure was last reviewed on 27 March 2021. However, the Procedure states that it should be reviewed on an annual basis. Upon review of the JOT Contingency Plan audit spreadsheet, we found that it includes a ‘library’ section and a review of the last updated date for a number of guidance documents. We found the following:   * 31/65 – last updated more than two years ago. * 4/65 – last updated between one year ago and two years ago. * 29/65 – guidance could not be found. However, it is noted that the majority of these guidance documents are not maintained by the Force or JOT, but outside agencies.   *Risk:* Insufficient and outdated guidance on contingency plans leads to an inconsistent approach towards emergency planning. |  |  | A role description is being drafted for consideration of advertising a full time post either seconded from Police or NFRS or recruited internally on a fixed term contract.  Ahead of the new JOT Homepage being delivered and as part of the above plan reviews any guidance on the JOT Homepage (no date set) will be removed if no longer relevant or referred to from the relevant plan.  28/05/2024 update.  Policy and Procedure documents are now under review with the first (Staff exposure to toxic hazards) having been completed and uploaded to the Policy Library. Both the Contingency Plans Policy & Procedure and Operational Order Policy & Procedure are under review against JESIP 3.1 Doctrine and should be updated by end of June 2024.  The LRF Testing and Exercising role has been successfully recruited into for maternity cover and a job description completed and TOR for that function within the LRF. |  |  |

**Reasonable Adjustments Follow Up – January 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| **3** | **Annual Review Process and Reporting**  Where Reasonable Adjustments are made for an individual, these should be reviewed on an annual basis to ensure they remain relevant and appropriate. Our previous audit report noted that the Force did not have any degree of oversight regarding the annual review timelines of the TRAAs that were in existence at the time. | As planned, the Force should review all TRAAs annually with the respective individual to ensure that the related reasonable adjustments are appropriate and effective in mitigating any disadvantage. | **3** | Since the previous audit we have created a dedicated HR Hub location for the secure storage of the TRAA’s. We have cleansed old TRAA’s and updated on the new TRAA format. We have limited the access to the TRAA’s to the passport holder, current line manager, and HR Advisor. This process | December 2024 June Withey, Workforce Planning Manager |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | During this audit, we note the development of the HR Hub, a dedicated platform in which the HR department stores all TRAAs in existence at the Force. We note that this includes details of each TRAA, including the date of review and their review status.  In addition, we reviewed evidence of an automated weekly email that summarises to the HR Department the number of TRAAs due for review.  However, we note that no updated TRAAs have reached the twelve-month requirement to be reviewed, and as such we were unable to confirm that annual reviews had been conduct appropriately.  As such, we were unable to confirm that the process in place for annual reviews is appropriate, and therefore cannot provide assurance that the process is effective.  However, the downgrade of the priority level reflects our assessment of the design of the controls in place with regards to annual reviews.  *Risk and Impact:* Reasonable adjustments are not regularly reviewed to assess whether they are still suitable, leading to unnecessary provision of reasonable adjustments or potential litigation where adjustments are inappropriate for an employee's requirements. |  |  | was completed in September 2023 therefore there is no current TRAA’s that are due for review. However, we are setting up a process to ensure that any TRAA’s that are due for review, and this will also mean the HR Business Support Advisor will have access to download the report to enable us to manage the review process. HR Business Support will run a monthly report from the HR Hub and contact passport holders via email to remind them that the TRAA they hold is due for review (or send a reminder if overdue). This process will commence mid 2024 due to the currency of the TRAA’s.  Update 13th Mar 24 – There is now a process in place where the Management Information Officer pulls a report from the HR Hub with details of TRAA’s that are coming up/due for review. This information is then passed on so that the passport/TRAA holder can review and update their TRAA. This is an interim process whilst awaiting the changes by DDaT to the TRAA section of the HR Hub to automate the review process. | Alison Roberts, HR Business Partner |  |
| **5** | **Benchmarking Activities are not in Place.** Benchmarking activities are a useful tool in ensuring that current working practices are consistent with legal and regulatory requirements, as well as being aligned to well performing peers.  Since our last audit, we were advised by the HR Business Partner that no progress has been made with regards to benchmarking, given the absence of developed KPIs. However, we were further advised that they will engage with the Head of Strategy and Innovation to identify opportunities for benchmarking. This is consistent with the Audit recommendation plan maintained by the Force.  *Risk and Impact:* The Force are unaware of the performance and appropriateness of their reasonable | The Force should ensure that benchmarking activity is conducted on a regular basis. This should be done by comparing the Force against peers, and any organisations producing best practice guidance such as the College of Policing | **3** | As stated above with regards to the KPI’s this is now in process. The HR Business Partner has contacted the Head of Strategy and Innovation and the force is reaching out to others forces to review what data is available and if this is comparable with Northants data. This will further support the ongoing development of the current KPI’s and support any development of the reasonable adjustment process.  Update 13/03/24 - We have with the assistance of the strategy and innovation unit gone out to other forces, who apart | March 2025 Alison Roberts, HR Business Partner  Sarah Peart, Head of Strategy and Innovation Unit |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | adjustments processes compared to peers and best practice, leading to instances of malpractice. |  |  | from the MET and Gwent, do not have KPI benchmarking for RA’s. They were all interested in the audit recommendations but at this point in time it is not a priority to undertake any further work in this area and therefore we will continue to use the KPI information that was originally presented to the People and Culture Board in November as part of the data pack. This can be revisited later in the year, but will be a separate piece of work around developing KPI’s. |  |  |

**Core Financials – March 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **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 and found:   * One instance where no request to raise the invoice could be evidenced. The invoice remains unpaid and overdue by 190 days at the time of the audit. * Two instances where the invoices had not been raised in a timely manner (18 days and 12 days).   We reviewed a sample of ten NCFRA debtor invoices and found:   * Nine instances where the invoices had not been raised in a timely manner (range of 45 – 12 days and average of 22 days). * One instance where the invoice remains unpaid and overdue by 82 days at the time of the audit. | Northamptonshire should ensure that invoice requests 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. To do this Finance Operations should not raise an invoice until a valid request is received.  Northamptonshire 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.  Northamptonshire should ensure overdue income is appropriately chased in line with debt management procedures. To do | **2** | Agreed - The process needs to be refined and better followed.  Update May 2024 – The recommendation is factually incorrect as Finance Operations do not receive the requests to raise a Sales Invoice this is completed currently in the finance management accounts team, Suzanne Clapp being the manager. This is under review to where this process should be completed to improve the process and adding value with best practice for Debt management.  There has vast improvements put in place for the information provided by the management accounts team for Team Leader in Finance Operations to chase any aged debt or any invoice due for payment. Debt Management procedures have been reviewed and the issues within the system | 01 April 2024 Nick Alexander / Debbie Clark  Revised date 30  September 2024 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | We were advised by management that there is no formal timeline in place for the 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. | this there should be clear oversight within Finance of all overdue income and evidence of debt chasing carried out at the required time intervals should be retained. |  | are being currently resolved. These will be complete for the next audit in September. |  |  |
| **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.  We reviewed a sample of 10 debtor invoices at the Force and five at NCFRA to confirm that aged debt processes had been followed in accordance with the procedural document. We found:   * Force – four instances, which were salary overpayments, where debt procedures had not been followed. This was due to there being no contact details on the individuals account for the Force to use following the no responses from the letters posted to their addresses. These debts remain overdue since Jan 2022 (three instances valued at £2920.51, £3275.81, £3987.55) and October 2022 (one instance valued at £2282.38). * Force – two instances where debt procedures had not been followed in accordance with the Process document. From a review of the October aged debt report we noted that verbal communication with | The Force 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 chase in accordance with timelines in the Aged Debt Process.  The Force should ensure that customers are set up with all necessary contact details including email address, phone number and home address. These should be kept up to date to allow for debt procedures to be followed in the event of the Force being owed money.  NCFRA should ensure that the Aged Debt Process is followed, by ensuring there is sufficient oversight of overdue income and clear escalation procedures in place, and documented evidence of agreed payment dates with customers is retained and can be evidenced upon request. | **2** | Agreed – Whilst the team has been very successful in driving down outstanding debts, a more robust process will ensure that issues do not arise again.  Re point 5: We believe this was the result of imported customer files, whereas in Unit4, all new customers are required to have all necessary details populated prior to raising any invoices.  Update May 2024 - The review of Aged Debt has taken place for year-end statutory accounts timelines. The Aged Salary overpayments within Police have been included in the review of Aged Debt for the Bad Debt Provision. Those migrated from MFSS have been written off if no details are held to chase the debt, a report is produced for every request to write off debt in line with the values for sign off in accordance with Financial regulations. Information now provided for new invoices has also improved as this is review by the Team Leader in Finance Operations before the debt is due.  The details for new customers has improved with additional information being added to the system.  Improvements for information received by verbal communications with customers is now documented on the Aged Debt Report which provides everyone visibility of the information held for the history of the debt | 01 April 2024 Nick Alexander / Debbie Clark |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | customers had occurred, and a payment date had been agreed. However, the Force does not have documented evidence in respect of this.   * NCFRA – Two instances where debt management procedures had not been followed in accordance with the Process document. Of these two instances, we did note one had now been paid, although this was two months late, and one instance (valued at £57,583.75) remains unpaid since July 2023 due to the invoice being rejected 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.  The Force does not have adequate contact details for employees with salary overpayments leading to a lack of avenues to use to chase overdue income resulting in financial loss to the OPFCC. |  |  | being chased. This document is reviewed in the Aged Debt meeting with both the Chief Finance Officer for the OPFCC and Police Chief Finance Officer.  NCFRA and Police follow the same procedure to ensure the process is followed robustly. |  |  |
| **3** | **NCFRA - Comparison of Employee Bank Details and Supplier Details**  The Force performs quarterly comparisons of employee bank details with supplier details and duplicates testing of employee bank details to identify instances where they match and therefore require investigation.  Whilst we noted no issues with Force procedures, we were not provided with evidence to demonstrate that NCFRA perform routine comparisons of employee bank details with supplier details.  Therefore, NCFRA should ensure that there is a preventive control for the detection of matching bank details between suppliers and payroll.  It is noted that this may be difficult due to the payroll function currently being outsourced to West Northants Council for NCFRA employees, therefore a detective control would be required to be regularly carried out to ensure instances are flagged appropriately and in a timely manner.  *Risk and Impact:* Fraudulent activity is not identified or prevented in a timely manner | NCFRA should implement regular and routine checks of employee bank details and supplier details, similar to the Force arrangements | **2** | Agreed – this control will be aligned to Police when payroll comes in-house  Update May 2024 – This is now part of month end processes and reviewed monthly | 01 April 2024 Nick Alexander / Sue Fisher |  |
| **4** | **NCFRA Leavers Access to Unit4** |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | NCFRA should manually end leaver’s access to the finance system, Unit4,, by moving their status to parked, following their leaving date.  We performed a population test of all leavers from NCFRA since April 2023 to confirm their system access had been removed in a timely manner. We found five instances from a population of 21 NCFRA leavers who still had active access to Unit4 despite having now left NCFRA.  We were advised by management that whilst the Force’s process in respect of ending leavers access to Unit4 is automatic, NCFRA do not have a HR system within enabling services as the Payroll/HR function currently sits with West Northants Council therefore a manual process is in place for the Force to end NCFRA leavers Unit4 access.  *Risk and Impact:* NCFRA leavers system access is not removed on a timely basis from Unit4 leading to inappropriate users accessing systems with confidential information and potential for data breaches resulting in reputational damage. | NCFRA should ensure that leaver’s Unit4 system access is removed in a timely manner following their leaving date. HR should notify IT of this requirement for a leaver on or before their leaving date.  In light of the planned integration between NCFRA and the Force, the Force should look to embed NCFRA into their HR system to enable the automation of ending leaver’s system access to Unit4. | **3** | Agreed – this was a temporary issue due to the conscious decision to not align the Finance and HR implementations of Unit4, and a workaround was not put in place promptly. This issue will be resolved with Unit4 for HR is implemented, as is part of the core design.  Update May 2024 - The new on-premise Unit4 HR system for NCFRS went live on 2nd April 2024. As a result, the leaver process now aligns to the leaver process for Northants Police, managed by the Enabling Services HR Team, who terminate leavers in Unit4. Notifications will be generated by the system and will be sent to the relevant departments. | 01 April 2024 James Swindall |  |
| **5** | **Supplier Amendments**  Amendments to supplier details arrive through a supplier request form to the Finance Operations e-mail inbox and the amendments request are verified with the supplier verbally over the phone or via email.  Once verified, Finance Operations will apply the amendment in Unit4 attaching backing documents, such as the supplier request, to support the amendment. This flows through workflow in Unit4 to a team leader in Finance with approval access to approve the amendment to the supplier details.  We reviewed a sample of ten supplier amendments at the Force and noted one instance (GS-51564) where workflow evidence to demonstrate segregation of duty between the inputter and approver of amended supplier details could not be provided.  We were advised by management that a workflow system error message associated with this sample was preventing them from demonstrating the required evidence. | The Force to review this instance, ensure the workflow system error is resolved and confirm appropriate segregation of duty is present in the supplier amendment made | **3** | This is an isolated incident regarding a transaction early in the use of Unit4 workflows. It is not expected to reoccur and to continue investigation is not good value use of our resources, but any future errors will be flagged and escalated to Unit4 experts for review. | N/A |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | *Risk and Impact:* The Force is unaware of system errors preventing the Force from ensuring all amendments to supplier details are appropriately reviewed and verified. |  |  |  |  |  |
| **6** | **NCFRA Petty Cash – Imprest Account Policy** NCFRA has a Petty Cash – Imprest Account Policy (April 2021) in place which documents the financial petty cash and Imprest requirements responsible NCFRA personnel must follow. This includes security requirements of petty cash, petty cash monetary restrictions and reconciliation and management review of petty cash records.  The NCFRA Petty Cash – Imprest Account Policy was last updated April 2021 and was due next for review April 2022. Therefore, the Policy is outdated and requires its annual review.  *Risk and Impact*: The NCFRA Petty Cash – Imprest Account Policy is outdated and is not fit for purpose leading to inconsistent approaches to the management of cash and cheques received into the NCFRA. | NCFRA should ensure that the Petty Cash – Imprest Account Policy is updated and approved at the earlier opportunity and reflects current petty cash working practices in place at NCFRA. | **3** | Agreed – policy to be reviewed and updated.  Update May 2024 – There is still an ongoing review by Ro Cutler for the petty cash in NCFRA.  Update July 2024 – The petty cash policy has been removed from Fireplace and is no longer used. | 01 April 2024 Nick Alexander / Debbie Clark / Sue Fisher |  |

**Vetting – March 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| **1** | **Vetting Documentation**  According to the Authorised Professional Practice (APP) on Vetting, clearance should not be granted to a vetting applicant until all relevant vetting enquiries have been completed. Additionally, Force Vetting Units should ensure that supporting documentation for checks undertaken should be maintained on the vetting file, such as copies of identification documents. From review of a sample of vetting applications, renewals, and appeals, we identified the following:   * Vetting applications – two out of 15 cases fingerprint and / or drug test results were still pending on CoreVet despite clearance being | Dip sampling should be undertaken on vetting files to confirm that adequate supporting documentation has been uploaded.  Procedures should be updated detailing when vetting clearances can be granted for applicants who have pending biometric vetting checks. | **2** | The vetting team leader will be dip sampling 10 files a month to ensure all documents including Bios have been uploaded to the file. The team leader will diarise the sampling as a reminder to conduct the checks.  Update 13/05/24 - This has now been implemented with checks commencing in April. | Force Vetting Manager  30 April 2024 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | granted. However, it is noted that biometric vetting is not a legal requirement according to the APP.   * Vetting renewals – one out of 10 cases the Decision Rationale Form (DRF) which is completed by the Vetting Officer with justification for granting clearance could not be located on CoreVet. * Vetting appeals – one out of 6 cases the initial request email / letter from the vetting applicant to initiate an appeal could not be located on CoreVet.   *Risk*: Inconsistent processing and documenting of vetting applications, renewals and appeals leads to the Force not being in compliance with the APP on Vetting and inadequate checks being undertaken on vetting applicants. |  |  |  |  |  |
| **2** | **Timely Processing of Applications and Renewals** Although there are no specific SLAs noted within the APP on Vetting, having clear targets in place in relation to the processing of vetting requests such as clear timescales can aid in ensuring that there is a sufficient level of accountability within the Vetting Team, and to help the Force in assessing the capacity needed to meet its vetting processing targets.  The Force has a number of targets in place for processing vetting requests and appeals. Vetting applications and renewals should be processed within 5-7 weeks, depending on the type of application, and vetting appeals should be processed within 2 weeks. Vetting performance information is reported on a monthly basis via email circulation and at quarterly Performance & Tasking meetings, however, the timeliness of processing applications is not reported on.  We reviewed a sample of 15 new requests, 10 renewals and 6 appeals and found that that the following were not processed within seven weeks:   * 2 out of 15 new applications * 3 out of 10 renewals | Performance reporting should include the timeliness of processing vetting applications, renewals and appeals. | **3** | The weekly performance figures will now include the turnaround times of applications.  The renewals will remain as they are. The current process being that the renewals are flagged 3 months prior to expiry to allow enough time for the applicant to respond and checks to be conducted prior to expiry. The time the checks take to clear is not a priority as long as the checks are completed prior to vetting expiring.  Update 13/05/24 - This has now been implemented, no change in response to renewals. | Force Vetting Manager  19 April 2024 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | *Risk:* The Force does not report on the timeliness of processing vetting applications, hindering the Force’s ability to allocate staff and budget appropriately to meet the demands of the vetting workload. |  |  |  |  |  |
| **3** | **Appeal Oversight**  Upon the rejection of a vetting application, the applicant may submit an appeal to the Force and request a review of its decision. Appeals are reviewed by an individual who is independent of the original decision-making process, typically the Force Vetting Manager (FVM). In some circumstances the appeal may be reviewed by another Force where the FVM has had some involvement in the original decision-making process.  Through our review of the Force’s weekly vetting performance reporting and quarterly reviews, we noted that the Force does not currently have any reporting arrangements in place to monitor its performance in relation to vetting appeals.  Best practice across the sector is to report on the number of appeals upheld and overturned as this provides an indication of whether vetting requests have been initially assessed correctly.  *Risk*: The Force does not have sufficient oversight of the vetting appeals process leading to it not being aware of the adequacy of the appeals process and effectiveness of its decision-making. | The Force should include performance indicators related to vetting appeals within its weekly and / or quarterly vetting performance reporting, such as outcomes of appeals and the timeliness of appeals being processed. | **3** | Vetting figures are collated quarterly to monitor numbers and disproportionality. The appeals have been added to the quarterly report and now include the outcome. All appeals are currently conducted within 10 working days. The time taken to respond to appeals will now be added to the report.  Update 13/05/24 - This has been implemented. | Force Vetting Manager  30 June 2024 |  |

**Fleet Management Follow Up– April 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| **4.1** | **Replacement of Vehicles**  *Observation:* From a review of the Vehicle Replacement Policy Schedule 2020-21, Audit noted there is a guidance document which indicates the replacement interval for each vehicle model, based on the vehicle life and the mileage with no vehicle having a vehicle life beyond 10 years. However, the schedule mentions that | The Force should clarify their position regarding their priorities to older vehicles, whether this is to ensure that the maximum utilisation is obtained from the vehicle or whether priority is to | **3** | The Replacement Policy is a guide in place to assist with the replacement programme. There will always be more than just one factor to consider before a vehicle will be replaced. Since COVID and Ukraine war we have worked within considerably tough | April 2024 Theresa Cheney |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | certain vehicles, namely Response and Neighbourhood vehicles, will be reviewed at 100,000 miles so that it is not necessary that the age of these vehicles will be given priority, as mileage is considered the cost- effective parameter.  Audit reviewed the list of vehicles that the Force has in the fleet and noted 46 vehicles that were older than 10 years. All 46 vehicles were raised with management, and it has been noted that these are pending replacement.  From a review of 23 of these vehicles, it was noted the Force has either replaced, is planning to replace, is salvaging or auctioning 16 of these vehicles. For the remainder of vehicles, the Force had a sound reasoning why vehicles were being retained, including vehicles that are being used as training vehicles but with mileage in excess of 100,000. However per the current guidance retaining vehicles beyond ten years is contrary to the guidance provided in the Vehicle Replacement Policy.  Moreover, through discussions with the Head of Transport, it has been noted that the Force intends to replace vehicles pre-2015 due to the changes in the regulations relating to emissions under the Road Vehicle Emission Performance Standards. However this is not currently factored into the existing Vehicle Replacement Policy.  This recommendation was raised during our August 2020 audit and we have noted that the Vehicle Replacement Policy 2023-24 still does not provide clear guidance on the management of older vehicles, therefore this is considered as not implemented.  *Risk:* The Force are unable to demonstrate alignment to their carbon emission objectives, through the retention of older vehicles.  Non-compliance of the guidance provided in the Vehicle Replacement Policy, as the vehicles used for training are over 100,000 miles. | be given to the tailpipe emissions objectives.  Once a clear approach has been agreed, a longer term replacement schedule should be drafted to support the future capital requirements to meet the fleet replacement needs. |  | supply chain’s/ increased costs and extended vehicle delivery dates and to further complicate this we have had a whole mixture of shift changes, single / double crewing and new departments formed very quickly, so the need for flexibility was essential and I would argue brought real value not risk. Further to this we cannot work on a longer term replacement schedule as our specialist response vehicles will achieve over 100,000 miles in 2 to 3 years and we cannot plan for accident write offs which become part of the replacement programme at any time. We can demonstrate that we have improved carbon emissions monitoring not only on our Fleet but all aspects of travel within the Force and our Fleet have vastly improved its age profile from its previous audit. We can also provide justification and reasons why we have extended the life of a vehicle to provide a core resource in the Force be that for a training requirement, additional resource for an additional department or a vehicle role profile for specific policing purposes. |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| **4.2** | **Vehicle Service Schedule Guidance – Motorbikes** *Observation:* The Force has a Vehicle Service Schedule Guidance document in place which notes when specific vehicles require a service based on both mileage and timeframe parameters. The document categorises vehicles based on their use to the Force and currently includes seven categories of vehicles. Such parameters have been set by the Force and are different to parameters set by manufacturer servicing guidance.  Review of the Vehicle Service Schedule Guidance document shows no guidance for frequency of servicing Force motorbikes.  We queried this with management who informed us that the Force only maintain a small number of motorbikes (roughly 15), and that servicing of these vehicles is in adherence to the respective manufacturers servicing guidance, as opposed to Force-established parameters.  *Risk:* Staff are unaware how frequently Force motorbikes should be serviced leading to inconsistency. | The Force should update the Vehicle Service Schedule Guidance document to include coverage of servicing guidelines for Force motorbikes, clearly indicating the key parameters that dictate the frequency of such services | **3** | The Vehicle Service guide has been updated to incorporate motorbikes and they have also been added to the scheduling module within Tranman. | April 2024 Theresa Cheney |  |
| **4.3** | **TranMan Record**  *Observation*: A physical job card is generated each time a vehicle is repaired/ serviced or subject to MOT at the Force’s workshop. Details captured include the vehicle registration, mileage, the reason why the vehicle has been called into the workshop and details of the work undertaken. Contents from the physical job card must then be manually inputted into the TranMan system. Audit selected a sample of 10 vehicles to confirm the details held on TranMan of the most recent service, MOT and corresponding mileage were consistent with that of their physical job card. We noted the following exception:  - 1 out of 10 cases where the mileage was recorded incorrectly on TranMan (vehicle registration – AX22 DXF).  For the above exception, the mileage as per the physical job card was 5,108 and was incorrectly recorded on the TranMan system as 6,108.  *Risk*: Records held on the TranMan system are not accurate, which could render the servicing and | The Force should ensure that details are inputted to the TranMan system accurately, as the Force utilises the system to co-ordinate the servicing programme | **3** | Whilst there will be occasions where vehicles fall outside of our service guidance mileages, they will still fall under the manufacturers requirements. All BMW’s are fitted with CBS (condition based service) lights and should these activate, the vehicle will be stood down and brought to workshop immediately for an oil change, these monitor the condition of the oil in the vehicle at all times. Due to the nature of our business the risk factor of not providing our specialist vehicles to perform their core role of protecting the public of Northamptonshire is far greater. The safety of our Officers is paramount and as such the vehicles are maintained to the highest standard and well within any manufacturer requirement.  As for inaccuracies on input of mileages on job cards there will always be an element of human error in any administration | April 2024 Theresa Cheney |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | maintenance programme ineffective, as services will not be undertaken at the right time. |  |  | process, but we are confident that we have sufficient fail safes in place to highlight an error such as service is due stickers in the vehicles, vehicle checks done on a weekly basis and the service schedule module that has a separate mileage input field. Whilst an automated system would be welcomed with the job cards being completed online and removing paper copies this would not stop human error completely as this would also rely on an element of administration by the technician completing the job. |  |  |

**Payroll – May 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| **1** | **Expenses are not validated or approved prior to their payment**  *Observation:* The Force's Expenses and Allowances Policy, which was last reviewed 21 January 2021 (**See recommendation 2)**, outlines that expenses will be reimbursed if the expenditure incurred in the course of duty is:   * Supported by a receipt * Of a reasonable amount * Necessary * Additional to what would have been normally spent   The policy also outlines that "Managers/ Heads of Departments and Area Commanders need only approve claims where queries are raised by the Payroll, HR or Finance functions or the claim is outside of the standard claim processes outlined within this document and require approval prior to submission.  Expenses are claimed through the Self Service Expense Claim within Forcenet. We reviewed a sample of ten expense claims made between April 2023 to August | The Force should ensure that expenses claims are formally approved and validated prior to their payment, with an audit trail retained to evidence the value and nature of the expense claimed.  The Payroll team should ensure that they receive confirmation to support the validity of expenses claims prior to their payment. | **3** | The risk of retrospective review is accepted and noted, however, the position remains that the Force’s policy is that inappropriate claims will be managed through PSD and HR and a full reimbursement would be expected. It is anticipated that with the appointment of an additional role under the Finance and Resources Officer we will be able to ensure a wider coverage and review of all claims, which will reduce the risk of those claims being unchallenged.  Update July 2024 - We now have a member of staff and undertake audits on a wider range of the expense claims which we log. I have met recently with PSD and provide reports monthly to them.  Recommended for closure. | Michael Montgomery  31 March 2025 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | 2023 to ensure that they were legitimate, in line with the policy, authorised and paid in a timely manner. In each instance whilst we were able to confirm that payment was made in a timely manner, no evidence was provided to support the validity of each claim, or its approval.  We were advised by the Payroll Manager that expenses claims are not verified by the Payroll team, as outlined in the policy, and instead a regular audit is undertaken by the Finance Department on a sample of expenses claims to verify their validity. We conducted a walkthrough of the audit arrangements in relation to expenses and noted that there is no formalised approach to conducting the review. We were advised that each month a different expense type is focused on, with ad hoc selection of expenses claims for that month based upon instances that appear exceptional or abnormal.  We reviewed the audit log used to log and monitor expense audits and noted that the audit process consisted of requesting evidence from the individual claimant, or an explanation of the nature of the expense. None of the ten expenses selected in our sample had been audited.  As such, we note that there is no preventative control in place that approves or verifies expenses claims before they are made. We commonly see this included within a system workflow, wherein line managers must approve expenses claims prior to their processing by the payroll team.  For reference, the total expenses claimed by Officers as reported in July 2023 was £33,993, of which £5,292 related to food and subsistence and £6,849 related to mileage and parking.  *Risk:* Inappropriate expenses claims are made that are not in line with the Force's policy, and do not relate to bona fide expenses claimed whilst working on behalf of the Force. |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| **2** | **The Policy library includes out of date policies and procedures, and procedural guidance is not in place**  *Observation:* The Force operates a policy library which stores all the policies and procedural guidance for the organisation. This is available through the Force Intranet. We requested all policies and procedures in relation to Payroll and were provided with a number of different policies taken from the Force's policy library. We reviewed the policies provided and noted that three versions of the Expenses and Allowances, and Overpayments and Underpayments policies were available in the policy library, as well as two instances of the Overtime policy. In all cases the versions of the policies reviewed had not been reviewed in line with their review cycles, and we noted that the policy owner was not consistent across versions. In one extreme instance an Overtime Policy had an effective date of April 2007.  We raised this to the Payroll Manager during our review, who subsequently provided an updated version of the Expenses and Allowances and Overtime policies. Whilst we confirmed that the Overtime policy was last reviewed in April 2023 with a next review date of April 2024, the Expenses and Allowances policy had an effective date of June 2021, requiring review in June 2022. We were advised that the Expenses and Allowances policy was currently under review.  Additionally, we reviewed the Starter and Mover procedural guidance notes in place to support Payroll staff and confirmed that this outlined the approach for inputting starters and transferring movers within iTrent. However, we note that the Force does not have procedural notes in place which document the approach to inputting, reviewing and approving payroll related data for other common processes including leavers, deductions, and variations. At similar organisations these often utilise screenshots to illustrate the process in place, supported by commentary. We find that maintaining clearly defined procedural notes provides continuity in performing day to day processes, as well as supporting business continuity. | The Force should review the policy library to ensure that only the most up to date versions of each policy are available.  The Force should ensure that the Expenses and Allowances policy is reviewed on a timely basis, in line with its review cycle.  The Force should develop procedural guidance documents that outline the process for the input, review, and approval of Payroll related data within iTrent. Guidance should include version control to support a regular review of the process, ensuring it is reflective of current practice. | **2** | A review of the policy library by the Chief People and Finance Officers is being completed and all policies and procedures will be reviewed and where appropriate revised throughout 2024/25.  Update May 2024 - This is currently ongoing with collaboration across HR and Finance to look at updates and clarity where needed.  Update July 2024 – Discussions are ongoing in relation to this.  Update September 2024 – The Travel and Expenses Policy is currently being reviewed by SM and will be circulated for consultation once complete. The Pay and Subsistence Policy was updated in 2023 but it is still on the old template so this will be moved to the new template and reissued. | Suzanne McMinn & Nick Alexander  31 March 2025 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | *Risk:* Staff are unaware of the current processes in place relating to Payroll, leading  to inappropriate claims or requests which are not aligned to the Force's policies.  Payroll staff are unaware of operational processes, leading to an inconsistent and  inappropriate approach to processing payroll data. |  |  |  |  |  |
| **3** | **Access arrangements for iTrent are under review, and permissions are not formally reviewed on a regular basis**  *Observation:* At the commencement of the audit, we were provided with a permissions list extracted from the Force’s payroll system, iTrent. We note that this included all payroll staff as having “System Administrator” access. Subsequently, during the review the Payroll Manager provided an updated extract, which illustrated that these permissions had been reduced for payroll officers to “Payroll with HR admin”. However, through discussions with the Change Programme Manager we were advised that, as part of the ongoing integration with NCFRA, permissions were being reviewed to ensure that these are limited only to activities that are required by those staff members.  Additionally, we were advised that members of the payroll that leave the team are immediately removed from the Payroll system. We were able to confirm that a recent leaver from the Payroll team no longer had access to iTrent through review of access permissions before and after their cessation. However, we note that the Force do not formally review the permissions on a regular basis. We were advised that an annual review is undertaken of permissions within the HR system, Unit4.  *Risk:* Inappropriate access to the payroll system increases the likelihood that inappropriate payments are made, and/or fraudulent behaviour. | As planned, the Force should review access permissions within the Payroll system, iTrent, as part of the NFCRA integration project that is ongoing. Permissions that facilitate the inputting, amending, and deletion of payroll data should be limited to Payroll staff, as well as IT and MHR consultancy related staff to facilitate the operation and update of the system.  Permissions should be developed to ensure segregation of duties is maintained.  Access permissions to iTrent should be reviewed on an annual basis as part of the existing annual review of the Unit4 HR system. | **2** | Alongside the system access reviews that are completed quarterly, we will ensure that payroll access is independently reviewed to ensure segregation and appropriate scrutiny.  Update Sep 24 – Reviews are already in place. Discussion are ongoing regarding system reviews – recommended for closure. | Michael Montgomery | 30 June  2024 |

**Identity Access Management – June 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| **1** | **Lack of Periodic User Access Reviews** *Observation:* Regular user access reviews should assess whether the Windows Active Directory (AD) user base, responsible for managing logins, permissions, and authenticating access to associated applications, is accurate and that individuals have not been assigned unnecessary access.  A regular regimen of access reviews has not been established to determine the suitability of access privileges for Windows AD accounts.  *Risk and Impact:* Failure to implement regular access reviews can lead to individuals retaining unnecessary access to Windows AD and related systems, creating additional points of access to external attackers. | Each organisation should implement a regular (e.g. quarterly) regimen of Windows AD access reviews. Line managers should review the access of their staff and any other users such as partnership workers that they are responsible for. Any unnecessary access detected during these reviews should be removed from relevant individuals.  As the Force is implementing SailPoint across its employees, it should assess whether SailPoint could provide this service automatically. For users not covered by SailPoint alternative manual processes may be required proportionate to the risk. | **2** | This recommendation is broadly accepted by management as it is recognised that there are currently process in place to address this, they do not currently extend to this level of scrutiny. Therefore, although there will be oversight of this process within the annual information auditor plans and role (due to be implemented by the end of the 2024 calendar year), this in-depth level of scrutiny will be fully implemented once we have the correct JML and access controls processes in place which will be managed automatically via the implementation of ITSM tool in December 2025. The source information reviews (a required prerequisite) will begin when the new information assurance structure is in place, this will inform the data utilised within the ITSM tool.  25/07/2024 No further update.  Update 06/09/24:  The process is currently conducted in conjunction with the Information Assurance and Systems admin teams and due to resource constraints is limited to ad hoc reviews at this time. However the new structure will facilitate the coordination of the ROPA, the underlying access required and then the audits will be planned and executed by the new information audit team. | Trina Kightley- Jones, Head of Information Assurance  31 December  2025 |  |
| **2** | **Multifactor Authentication for Fire AD Accounts** *Observation:* Multifactor Authentication (MFA) provides additional layers of authentication beyond passwords, that attackers must also breach should passwords become known to them. Best practice frameworks such | NCFRA should continue the process of setting up MFA for Fire Service accounts, ensuring that all accounts are covered by this process. | **2** | We agree with the audit recommendation and acknowledge the importance of multifactor authentication for securing Fire Service accounts. As noted in the recommendation, we have started the process of implementing this security | Roy Cowper, Enterprise Architect  30 September  2024 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | 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. |  |  | measure for administrative accounts and on a per project basis. The intention  would be to enable this for accounts within EntraID. Full implementation will require executive support from the organisation and of other affiliated bodies.  We will commence this process, monitor the progress, and report any issues or challenges. A date has been set of 30/09/2024 subject to approval by the organisation.  Update 13/08/2024:  In progress, delivery dates not yet amended.  Update 06/09/24:  MFA - Currently in 28 day consultation with Fire, Lisa Jackson to advise of consultation outcome. |  |  |
| **3** | **Privileged Access**  *Observation:* Privileged Identity Management (PIM) should, according to the time-restricted access policy configured in the PIM tool, provision privileged roles to individual users for a specified period before being withdrawn automatically.  Within the Police Azure tenant access to privileged accounts is controlled on a timerestricted basis, with higher privileges being assigned for shorter periods of time. While some low-level privileges are assigned to users permanently this has not been viewed as a risk due to their extremely limited capabilities. Within the Fire Azure tenant a similar system has been implemented, however time-restricted access has not yet been applied as strictly, with some medium-level privileges being assigned to a number of fire user accounts permanently. We were informed by management that such privileges should only be provided on a time limited basis and thus require review. | Each organisation should align the privileged access management procedures to ensure that where possible a principle of least privileged is followed when assigning access to user accounts.  Privileges assigned to users on a permanent basis, such as those assigned to users in the Fire Service Azure tenant should be reviewed and if possible, removed, such that they can be reassigned on a temporary basis to apply specific authorised changes. | **2** | We acknowledge the audit action and agree that privileged access management is a key aspect of ensuring cybersecurity. We have reviewed the privileges assigned to users in the Fire Service Azure tenant and some work has already been completed to bring key AzureAD roles under the control of PIM. We have removed permanent privileges that didn’t require escalation and established a process for requesting and granting them on a temporary basis when needed. The process of bringing the Fire tenant up to the same level as the Police tenant in respect of this security control will continue as part of business as usual. A date has been set of 30/09/2024.  25/07/2024 No further update. | Roy Cowper, Enterprise Architect  30 September  2024 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | *Risk and Impact:* Privileges assigned to accounts on a permanent basis may be used to apply unapproved changes without management oversight. |  |  |  |  |  |
| **4** | **Password Management Tool Implementation** *Observation:* It is good practice to use a password management tool to secure the passwords for generic administration and service accounts in order to prevent their exposure through the use of less secure password storage methods.  A password management tool has not been implemented for Police Service AD service accounts, whilst for Fire Service accounts a tool has been implemented but which only contains passwords for a small minority of accounts.  *Risk and Impact:* Passwords may be documented in insecure locations such access to relevant accounts may be achieved the event of a security breach*.* | Each organisation should store all generic administration and service account passwords in a password management tool. | **2** | This recommendation is accepted and there is a PAM (Password Access Management) Project in progress that is being led by the Transformation and Change team with a project manager assigned. Budget has been allocated and we have collated requirements which include the ability to store all generic administration and service account passwords, and supplier demonstrations have now taken place. This will be reviewed bi- monthly to ensure progress is made.  Update 25/07/2024 VS:  All requirements are done and quotes obtained, and business case is in development. | Andrew Jones, Head of Transformation and  Change  31 March 2025 |  |
| **5** | **Completion of Access Changes**  *Observation:* Changes to access should only occur on supply of a proper request.  The OPFCC, Force and NCFRA were unable to provide relevant documentation to support the completion of access changes as follows:   * For five out of eight joiners, a HR notification form was not available. * For one out of eight joiners, evidence of vetting and training was not available. * For all eight leavers, a HR notification form was not available.   *Risk and Impact:* User accounts may be created or disabled without proper justification. | Emails and other documents supporting access requests should be automatically attached to tickets raised to the service desk. If this is not feasible the access management procedures followed by the service desk should state that all such emails/documents should be manually attached to relevant tickets and relevant staff made aware of this requirement | **2** | This recommendation has been reviewed and has been accepted. Although tickets are already created from HR data, this process will now be reviewed to identify the capability of the current HR hub, ITSM tool and automation, if that cannot be easily done within these existing platforms then this will be developed with the new ITSM tool. The associated action will be to review this and report to key stakeholders.  Update 11/07/2024 DC:  The ITSM procurement phase is well underway, due for completion August/September 2024. | Dan Cooper, Head of Technical Support  01 July 2024  December 2024 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  |  |  |  | Update 24/07 DC - We have undertaken a review of the capabilities of both ITSM Police and Fire ITSM solutions and neither have the ability to manage access requests in the method described.  We are in the process of procuring a new ITSM joint platform, the procurement process is due for completion next month, where we will work with the supplier to understand if the data we receive from HR in the JML process can be used to provide both organisations with a higher level of audit capability in this area.  The new ITSM platform is unlikely to be made live until the next financial year.  Update 13/08/2024 (YH)  Discussed with CDO as procurement is still ongoing and implementation likely to be Autumn 24. Request to adjust delivery dates in line with ITSM revised implementation.  Update 06/09/24: (YH)  Due to procurement activity and delayed ITSM implementation request for these dates to move to March 2025 |  |  |
| **6** | **Monitoring and Logging Policy**  *Observation:* A specific IT policy should set out the organisational requirements for monitoring and logging, this should be used to guide the operations of the IT team as well as to inform regular users of any responsibilities regarding the monitoring and logging process.  A specific monitoring and logging policy detailing requirements and procedures for access monitoring and information logging has not been developed. Some requirements, such as the logging of multiple failed password attempts, have been added to the information security / access control policies, however | Each organisation should devise a monitoring and logging policy, including necessary ownership, version control and review sections. Once approved it should be communicated to those individuals that perform security monitoring and configure security logs. | **3** | We agree with the audit action and recognise the importance of having a clear and updated policy for monitoring and logging. We will allocate a task to  develop a draft policy that defines the objectives, scope, roles and responsibilities, frequency, and procedures for monitoring and logging.  25/07/2024 No further update. Update 06/09/24: | Roy Cowper, Enterprise Architect  30 September  2024 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | 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. |  |  | Logging and Monitoring Policy (Identity Access) is not the same as the IT Asset Management Policy (IT Asset Legacy Management). On track, this policy is in development and is being written by Simon Creasey (Digital Security Architect), draft to be shared by the end of the month. |  |  |

**IT Asset Legacy Management – June 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| **1** | **Automated scanning of hardware and software is not used to identify inaccuracies in the IT asset register.**  *Observation:* Automated scanning of hardware and software enables organisations to identify discrepancies between the IT asset register and devices present on their network.  The Head of Digital, Data and Technology confirmed that there is currently no software in place to scan the network for discrepancies between the IT Asset Register and the actual devices deployed across the Force. Northamptonshire Police & Fire are currently in the process of purchasing a new IT Service Management (ITSM) tool, which we are informed will include this function, with the intention to begin implementation from May 2024.  Furthermore, dependent on their type, most devices are separately managed by other software; for example, laptops are registered by Intune, however apart from a historic feed from the Blackberry management software for mobile devices, there are no other automated updates to the IT asset register to keep it updated.  *Risk and Impact:* Inaccuracies in the IT asset register, such as those that arise from failure to apply manual updates of new devices, prevent effective management | Continue with the planned implementation of a new ITSM tool that includes device scanning to identify discrepancies with the IT Asset Register.  Once implemented the software should also consume feeds from the management software for each class of device.  IT asset register discrepancies identified by automated scanning or following receipt of information from device management software should be investigated before their application to the IT asset register | **2** | The procurement and implementation of the new ITSM tool is ongoing and DDaT will implement the software in three phases, starting from the first quarter of the current fiscal year and ending by the fourth quarter of the next fiscal year.  The first phase will involve installing and configuring the software on the servers and integrating it with the existing IT systems. The second phase will involve testing and validating the software functionality and performance, as well as training the staff on how to use it. The third phase will involve deploying the software to all the devices and conducting a post- implementation review.  The current system does not provide Integrations required to consume feeds, however these capabilities are present in the new tool.  In the meantime, we are currently exploring opportunities to see how the reporting tools can help us determine device usage. The initial goal is to identify devices not in use against our asset lists.  Update 11/07/2024 DC: | Dan Cooper, Head of Technical Support - DDaT  31 December  2025 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | of the Northamptonshire Police & Fire devices, whether this be from a financial, security or service management perspective. |  |  | The ITSM procurement phase is well underway, due for completion August/September 2024.  Update 13/08/2024 (YH)  Discussed with CDO as procurement is still ongoing and implementation likely to be March 2025. Request to adjust delivery dates in line with ITSM revised implementation. | December 2024 |  |
| **2** | **Formal reviews of the IT asset register do not take place**  *Observation:* Regular reviews of the IT asset register should be conducted to verify that the information within the register is complete, accurate and up to date. Management confirmed that reviews of the IT asset register do not take place and there is currently no plan to implement a formal review.  *Risk and Impact:* Omissions and inaccuracies in the IT asset register could lead to incomplete application of security controls or assessment of security risks, which may cause a vulnerability to be unresolved that is exploited in a subsequent security incident. | Implement regular (e.g. quarterly) reviews of the asset register, to check that information in the register such as assigned user is accurate. Whilst automated scanning can support this, other checks to confirm that manual updates have been correctly applied should occur.  For example, periodic stocktakes of devices in storage, discovery of devices that have not connected for a long period, and verification of disposal are all activities that could occur to support the accuracy of the IT asset register. | **2** | DDaT agrees with this recommendation and will review the asset register regularly, to make sure information like assigned user is correct. The technical support team manages the IT Asset register and has started a quarterly dip sample process. | Dan Cooper, Head of Technical Support - DDaT  Complete |  |
| **3** | **Assessments of IT infrastructure risks are performed on an ad-hoc basis**  *Observation:* IT infrastructure should be subject to formal periodic review to assess its adequacy and highlight any risks that are not identified through day- to-day management activities.  We noted periodic assessments of the infrastructure do not take place, instead risks are identified in the course of normal management activities. We found only three risks relating to infrastructure support had been identified and assessed, with these risks covering software upgrades, Cyber Security and ageing systems, | Periodically assess the adequacy of IT architecture to identify and locate potential risks. | **3** | DDaT accept the recommendation. The Enterprise Architecture team are in the process of developing a suite of roadmaps.  The infrastructure roadmap  was developed in late 2023 and is designed to account for a number of identified risks. These risks will be captured in the register more formally going forward. These risks will the then be managed in line with our existing risk management processes. | Roy Cowper, Enterprise Architect – DDaT  31 December  2024 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | 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 |  |  | In addition, we are about to enter a procurement process for an Enterprise Architecture tool that will bring together all the information from multiple sources inclusive of risks, contract end dates, the solution / software catalogue and infrastructure components to enable better visibility of the IT Landscape.  25/07/2024 No further update. |  |  |
| **4** | **Two leavers had devices still assigned to them after leaving**  *Observation:* Any equipment assigned to staff should be returned to the organisation before leaving.  We tested a sample of 5 leavers to verify that the asset register had been updated to show the device is no longer assigned to them. We noted from testing that two of these leavers still had Blackberry phones assigned to them following their leave date.  Following this we identified that indeed 117 Blackberry phones are still distributed to staff, yet the Service Desk Manager confirmed that Blackberry devices are no longer in use, and some may not have been returned by staff. As a result, the IT Asset register has not been updated to show that they have been returned. We noted that Blackberry phones had been decommissioned in 2017, and we were informed that users have since been unable to access these phones since this point.  *Risk and Impact:* Mobile phones not collected from leavers could become avenues for inappropriate users to gain access to Northamptonshire’s network, potentially leading to confidential data being leaked and incurring costs for the organisation. As access to these Blackberry phones is now disabled this risk is however considered minimal. | Apply updates to asset register to reflect the true status of these Blackberry phones (i.e. lost) or arrange for their return.  If asset can’t be returned, then it should be treated as a lost device within the IT asset register. | **3** | As the Blackberry handsets are no longer connected to the network and the associated sims are from an expired contract, these devices hold no value and therefore all blackberry assets have now been marked as disposed or scraped. The two outstanding phones have now been marked as lost. | Dan Cooper, Head of Technical Support - DDaT  Complete |  |
| **5** | **A formal IT Asset Management policy/procedure document has not yet been implemented.**  *Observation:* An IT asset management policy is necessary for appropriate governance of IT assets acquired and managed by the Force. | As planned, publish an IT Asset Management policy setting out policy statements related to each stage in the IT asset lifecycle. | **3** | We agree with this recommendation and have initiated the process of developing an IT Asset Management policy that covers all the stages of the IT asset lifecycle, from | Dan Cooper, Head of Technical Support - |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | 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*.* |  |  | planning and acquisition to disposal and decommissioning.  The draft IT Asset Management policy is currently under review by the senior management team.  Update 11/07/2024 DC:  The draft policy is under review by the CDO.  Update 24/07/24 - An updated IT Asset Management policy has been through a first draft and is on a second re-write, looking to condense other policies pertaining to IT asset management, such as IT Equipment Disposal and Removeable Media Policies. I’ll begin to work on the next draft after my leave, returning 12th August, for resubmission to the CDO in preparation for the September CDO Board.  Update 06/09/24:  Approval in Fire needed. This will go to CDO board in Sept, then it will go to Fire for consultation process. Fire have a specific format. | DDaT  30 June 2024  30 September  2024 |  |

**2024/25**

**Grant Funding – 27 June 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| **1** | **Process of monitoring grant funding provided to grantees**  *Observation:* In the blue-light sector, it is best practice for grantees use of grant funding from the grantor to be monitored formally through quarterly monitoring reports where the grantee provides information and | Northamptonshire OPFCC should:   * Clearly set out and establish in funding agreements a quantifiable frequency for | **2** | It is pleasing to see that there are strong processes in place around this part of our business and a programme of work will be | Paul Fell, Director of Delivery, OPFCC |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | evidence on how funds have been spent to enable the grantor to check that grant funding has been spent in line with the funding agreement.  Monitoring arrangements should be clearly set out in funding agreements and the OPFCC should be proactive to collect monitoring information from grantees to enable early detection of instances where the grant funding has not been spent in line with agreements, including recovering any unspent funds from the grantee.  At Northamptonshire OPFCC, grant funding agreements state that “the beneficiary shall provide information requested in the format and within the timescales as the OPFCC reasonably requests from time to time.” Operationally, the OPFCC expects grantees to provide completed monitoring forms, attached with receipts and invoices as evidence of purchases made with grant funding, in Q1 of the following financial year (June 2024).  This poses the risk that the OPFCC does not obtain timely internal assurance that grant funding provided to grantees is being spent in line with grant agreements and approved grant applications, such as inappropriate purchases are being made or grantees spending is not sufficiently allocated across the timeline of the project. Also, this may cause issues in the OPFCC recovering unspent funding from grantees in a timely manner.  Additionally, we reviewed a sample of five grantees who have already provided monitoring reports and noted the following:   * One instance (Basketball Northants) where the monitoring form completed by the grantee and provided to the OPFCC does not include the required evidence of receipts and invoices for purchases made by grantee with grant funding (£6000). * One instance (South Northants Youth Engagement) where the grantee has provided their own format of a monitoring report which is not in line with the OPFCC required monitoring form and does not include the required receipts and invoices to evidence the grant funding spend (£3000).   *Risk and Impact:* The OPFCC’s grantee monitoring process lacks timely collection of monitoring | monitoring arrangements of grantees.   * Consider more frequent monitoring processes, such as quarterly monitoring forms or using the expected outcomes and target dates in grantee applications, to enable scrutiny of, and timely internal assurance over, the use of grand funding by grantees. This will be particularly useful for larger funding provided to projects taking place over a longer period of time. * Remind grantees submitting monitoring forms that they are to be completed via the official OPFCC monitoring form and all receipts and invoices for purchases made must be attached to evidence grant funding spend. |  | put into place to deliver against the recommendation | 30 September  2024 |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
|  | information from grantees which could lead to the OPFCC failing to identify, in a timely manner, any instances of grantee non-compliance with funding agreements.  Grantees do not provide the required monitoring information in monitoring reports, including receipts and invoices for purchases made, which could lead to the OPFCC being unable to validate that purchases made are in line with funding agreements and recover, in a timely fashion, any underspend of grant funding from grantees. |  |  |  |  |  |

**Regional Collaboration Audits 2023/24**

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

**2023/24**

**EMSOU – Capital Programme March 2024**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| **1** | **Funding of EMSOU Capital Programme**  EMSOU produces a Capital Programme each year as part of the budget setting process, which covers the budget for the upcoming year and a forecast budget for the following 3 years. This covers the expenditure from replacement of assets and the funding from grants, reserves and additional revenue contributions. Funding is then agreed at the PCC/CCs meeting, following recommendation from the CFO/FDs Board, as revenue funding from the Force for the upcoming year in their budgets.  Audit has reviewed the current Capital Programme and noted that reserves will be fully utilised by 2024/25 and therefore further funding will be required from the Forces.  HMICFRS have also found areas of concern in their PEEL 2021/22 review into Serious and Organised Crime. This noted concerns regarding the funding model for EMSOU as the PCC/CCs meeting couldn't agree on a three-year settlement, therefore leaving the Unit with the uncertainty of yearly funding.  *Risk and Impact:* The Unit is not able to replace or maintain current capital assets and is unable to fund the purchase of new capital assets. | The Forces and Unit should develop a Capital Programme to ensure that any future deficits in capital funding can be met. This should align to HM Treasury's three-year funding formula for serious and organised crime.  . | **2** | A revised Capital Programme will be produced that reflects the future Target Operating Model for the Unit and updated to include any future replacement costs for covert/control room equipment.  The Capital Programme will consider the funding requirement, funding options and guidance on any accounting arrangements – this will be built into funding discussions with CFO/FDs and reported back to the regional CC/PCCs Board | EMSOU Head of Finance and Corporate Services  30 September  2024 – subject to regional agreement on the Target Operating Model |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management response** | **Timescale/ responsibility** | **Status** |
| **2** | **Multiple Fleet Management Approaches**  The Unit uses around 150 vehicles, with about half managed by EMSOU while the remainder are managed by one of the five Forces.  This has resulted in different procurement and replacement strategies for the Unit's Fleet - a point that has been raised as part of the HMICFRS' review into EMSOU as part of the PEEL 2021/22 regional reviews into serious and organised crime. This identified a cause for concern where it would be more efficient to have a single capital replacement strategy and budget for the Unit, also allowing for savings to be made by adopting a regional approach to the procurement of vehicles and equipment.  *Risk and Impact*: Vehicles used by EMSOU are not appropriately maintained and/or replaced, increasing the risk of injury and/or death to the public, officers and staff. | The Unit should adopt a single fleet management approach to procurement and replacement of vehicles | **2** | A review of the fleet replacement process will be undertaken to consider any alternative procurement arrangements and whether this would deliver improvement in relation to:   * Purchase cost of vehicles * Service and maintenance arrangements * Fleet admin processes. | EMSOU Head of Finance and Corporate Services  30 September  2024 |  |

**EMSOU – HMICFRS Action Plan May 2024**

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