**INTERNAL AUDIT RECOMMENDATIONS DASHBOARD**

**Summary of Audit Outcomes**

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

**Northants Audits**

**2023/24**

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

**2024/25**

| **AUDIT** | **DATE** | **GRADE** | **RECOMMENDATIONS MADE** |
| --- | --- | --- | --- |
| **Priority 1** | **Priority 2** | **Priority 3** |
| Grant Funding | 27 June 2024 | Substantial Opinion | 0 | 1 | 0 |
| Medium Term Financial Planning | 18 September 2024 | Substantial Opinion | 0 | 0 | 0 |
| Asset Management | 30 October 2024 | Moderate Opinion | 0 | 1 | 3 |
| Joint Core Financials | 27 November 2024 | Moderate Opinion | 0 | 2 | 3 |
| Workforce Planning | 27 February 2025 | Moderate Opinion | 0 | 1 | 0 |
| Business Continuity & Emergency Planning Follow Up | 29 May 2025 | n/a | 1 | 0 | 0 |
| Procurement and Supply Chain | 18 June 2025 | Moderate Opinion | 0 | 2 | 1 |
| Joint Governance | 03 July 2025 | Moderate Opinion | 0 | 1 | 2 |
| Police and Fire IT Governance | 29 July 2025 | Moderate Opinion | 0 | 2 | 2 |
| Joint Estates Management | 22 August 2025 | Moderate Opinion | 0 | 1 | 0 |

**Summary of Audit Recommendations Progress**

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

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **2024/25 AUDITS** | **RECOMMENDATIONS MADE** | **RED** | **AMBER** | **YELLOW** | **GREEN** |
| Grant Funding | 1 | CLOSED |
| Medium Term Financial Planning | 0 | CLOSED |
| Asset Management | 4 | 1 | 0 | 3 | 0 |
| Joint Core Financials | 5 | CLOSED |
| Workforce Planning | 1 | 1 | 0 | 0 | 0 |
| Business Continuity & Emergency Planning Follow Up | 1 | 0 | 0 | 1 | 0 |
| Procurement and Supply Chain | 3 | 0 | 1 | 0 | 2 |
| Joint Governance | 3 | 0 | 0 | 2 | 1 |
| Police and Fire IT Governance | 4 | 2 | 0 | 2 | 0 |
| Joint Estates Management | 1 | 0 | 0 | 1 | 0 |
| **Totals** | **23** | **4** | **1** | **9** | **9** |

**OUTSTANDING RECOMMENDATIONS**

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

**2023/24**

**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. Anyunnecessary 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 alternativemanual 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 beimplemented by the end of the 2024 calendar year), this in-depth level of scrutiny will be fully implemented once we have the correct JML and access controls processes in place which will be managed automatically via the implementation of ITSM tool in December 2025. The source information reviews (a required prerequisite) will begin when the new information assurance structure is in place, this will inform the data utilised within the ITSM tool.25/07/2024 No further update.Update 06/09/24:The process is currently conducted in conjunction with the Information Assurance and Systems admin teams and due to resource constraints is limited to ad hoc reviews at this time. However the new structure will facilitate the coordination of the ROPA, the underlying access required and then the audits will be planned and executed by the new information audit team.Update 30/09/24 (YH)Consultation and recruitment underwayUpdate 31/10/24 (YH)Consultation now complete and largescale recruitment underway. DDaT are working with the comms department to facilitate an effective and targeted recruitment campaign to ensure these roles are filled. Update 31/03/25 – No changeUpdate TKJ May 25 - I've requested that this is the next audit we complete. The Audit Manager and Auditor have started. They have carried out an initial Locker Audit just to get in the swing of things so Audit activity will be in full swing soon. By 30/06 the audit will be underway by then or be in the process of reporting back to SIRO. | Trina Kightley-Jones, Head of InformationAssurance31 December 2025 |  |
| **2** | **Multifactor Authentication for Fire AD Accounts***Observation:* Multifactor Authentication (MFA) provides additional layers of authentication beyond passwords, that attackers must also breach should passwords become known to them. Best practice frameworks such as Cyber Essentials recommend that MFA is applied where available, and always for cloud services.Accounts within the Police Service Windows AD domain have MFA configured, however, the process to enable this for Fire Service AD accounts is still ongoing.*Risk and Impact*: Should the passwords for Fire Service user accounts be determined in a security attack, such as through the use of malware, these accounts could be accessed resulting a severe security breach that could be used to access data across the network. | NCFRA should continue the process of setting up MFA for FireService 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 therecommendation, we have started the process of implementing this security measure for administrative accounts and on a per project basis. The intentionwould 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 theorganisation.Update 13/08/2024:In progress, delivery dates not yet amended.Update 06/09/24:MFA - Currently in 28 day consultation with Fire, Lisa Jackson to advise of consultation outcome.Update 30/09/24 (YH)Lisa Jackson in Fire has confirmed that this consultation has been agreed in Fire. However following initiation of this work and further investigation by DDaT, a paper is being developed by the Digital Security Architect to consider the wider security considerations in relation to MFA and the holistic cyber security implications. This work should not be completed in isolation and there must be precursor work regarding security keys ect prior to the switching on of MFA in fire. A request for this action to be extended to Jan 2025Update 30/11/25 (YH)A request for this action to be extended to Jan 2025 has been approved. YH to send reminder to ensure work is progressing at required pace.Update January 25 - A request for this action to be extended to Jan 2025 has been approved. Digital Security Architect developing paper for approval. On track Update January 2025 - It has been confirmed that the ECF and Union have not yet agreed on complete MFA for Fire. The SLT meeting minutes state that MFA is not mandatory in fire and the action to progress it was closed. The CAF and digital standards recommendations highlight MFA in fire as a requirement. As a result, an additional paper will be written by DDaT Digital Security Architect. **Request to move date to 30th April 2025** for this work to be completed and approved to be sought.Update March 2025 - No approval for MFA in Fire provided by FBU. However, Project to provide personal devices to all fire staff now under review, SYAP and CAF recommendations highlight the need for personal issue devices which means this recommissioning is being picked up as part of that work now Request to move date to 31/12/2025 | Roy Cowper, Enterprise Architect30 September 2024January 202530 April 202531 December 2025 |  |
| **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 andservice account passwords in a password management tool. | **2** | This recommendation is accepted and there is a PAM (Password Access Management) Project in progress that is being led by the Transformation and Change team with a project manager assigned. Budget has been allocated and we have collated requirements which include the ability to store all generic administration and service account passwords, and supplier demonstrations have now taken place. This will be reviewed bi- monthly to ensure progress is made.Update 25/07/2024 VS:All requirements are done and quotes obtained, and business case is in development.Update 30/09/24 (YH)Currently in the commercial process for signing by the commissioner.Update January 2025 - The commercial activity has been placed on hold – Queries relating to Cloud viability now being explored as requested by stakeholdersUpdate March 2025 - The concerns regarding the Cloud viability have now been explored and a revised commercial request has been submitted for progression. The due date for this implementation will need to be revised to allow time for the procurement activity to take place, this is now an RFQ rather than the previous RFI. Due date to move to 01/10/2025 and to be monitored. | Andrew Jones, Head of Transformation andChange31 March 202501 October 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 followedby the service desk should state that all such emails/documentsshould be manually attached to relevant tickets and relevant staff made aware of this requirement | **2** | This recommendation has been reviewed and has been accepted. Although tickets are already created from HR data, this process will now be reviewed to identify the capability of the current HR hub, ITSM tool and automation, if that cannot be easily done within these existing platforms then this will be developed with the new ITSM tool. The associated action will be to review this and report to key stakeholders.Update 11/07/2024 DC:The ITSM procurement phase is well underway, due for completion August/September 2024. Update 24/07 DC - We have undertaken a review of the capabilities of both ITSM Police and Fire ITSM solutions and neither have the ability to manage access requests in the method described.We are in the process of procuring a new ITSM joint platform, the procurement process is due for completion next month, where we will work with the supplier to understand if the data we receive from HR in the JML process can be used to provide both organisations with a higher level of audit capability in this area.The new ITSM platform is unlikely to be made live until the next financial year.Update 13/08/2024 (YH)Discussed with CDO as procurement is still ongoing and implementation likely to be Autumn 24. Request to adjust delivery dates in line with ITSM revised implementation.Update 06/09/24: (YH)Due to procurement activity and delayed ITSM implementation request for these dates to move to March 2025Update 31/10/24 (YH)The procurement for the tool is progressing well. The revised project stage gates remain accurate.Update March 25 – The procurement for the tool is progressing, with contracts now signed. However, due to the extended nature of the procurement the delivery date for this action will need to be revised as well as the revised project stage gates, which will be communicated by the Head of Tech Support. The completion of the procurement is required before this action can be completed. Request to move date to 30/09/2025.Update May 25 - This will be delivered as part of the ITSM project due to go-live at the end of 2025. | Dan Cooper, Head of Technical Support01 July 2024December 202431 March 202530 September 202531 December 2025 |  |

**IT Asset Legacy Management – June 2024**

|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management Response** | **Timescale/ responsibility** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **Automated scanning of hardware and software is not used to identify inaccuracies in the IT asset register.***Observation:* Automated scanning of hardware and software enables organisations to identify discrepancies between the IT asset register and devices present on their network.The Head of Digital, Data and Technology confirmed that there is currently no software in place to scan the network for discrepancies between the IT Asset Register and the actual devices deployed across the Force. Northamptonshire Police & Fire are currently in the process of purchasing a new IT Service Management (ITSM) tool, which we are informed will include this function, with the intention to begin implementation from May 2024.Furthermore, dependent on their type, most devices are separately managed by other software; for example, laptops are registered by Intune, however apart from a historic feed from the Blackberry management software for mobile devices, there are no other automated updates to the IT asset register to keep it updated.*Risk and Impact:* Inaccuracies in the IT asset register, such as those that arise from failure to apply manual updates of new devices, prevent effective management of the Northamptonshire Police & Fire devices, whether this be from a financial, security or service management perspective. | Continue with the planned implementation of a new ITSM tool that includes device scanning to identify discrepancies with the IT Asset Register.Once implemented the software should also consume feeds fromthe management software for each class of device.IT asset register discrepancies identified by automated scanningor following receipt of information from device management software should be investigated before their application to the ITasset register | **2** | The procurement and implementation of the new ITSM tool is ongoing and DDaT will implement the software in three phases, starting from the first quarter of the current fiscal year and ending by the fourth quarter of the next fiscal year.The first phase will involve installing and configuring the software on the servers and integrating it with the existing IT systems.The second phase will involve testing and validating the software functionality and performance, as well as training the staff on how to use it. The third phase will involve deploying the software to all the devices and conducting a post- implementation review.The current system does not provide Integrations required to consume feeds, however these capabilities are present in the new tool.In the meantime, we are currently exploring opportunities to see how the reporting tools can help us determine device usage. The initial goal is to identify devices not in use against our asset lists.Update 11/07/2024 DC:The ITSM procurement phase is well underway, due for completion August/September 2024. Update 13/08/2024 (YH)Discussed with CDO as procurement is still ongoing and implementation likely to be March 2025. Request to adjust delivery dates in line with ITSM revised implementation.Update 30/09/24 (YH)Request to move dates accepted.Update January 25 – No change - On track.Update March 25 - The ability to address this action is reliant on the delivery of the ITSM tool. Request to move date to 31/09/2025Update May 25 - This will be resolved as part of the ITSM project where each piece of hardware will be tracked and records of software deployment will be maintained as part of the Service Catalogue. This is on track for the end of 2025. | Dan Cooper, Head of Technical Support -DDaT31 December 2025December 202431 March 202530 September 202531 December 2025 |  |

**2024/25**

**Asset Management – 30 October 2024**

|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management Response** | **Timescale/ responsibility** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **Lack of equipment and inventory checks***Observation:* The Force and the Service should ensure that regular equipment inventories are taken to ensure operational readiness, to ensure that all the necessary equipment is available and in proper working conditions in preparation for an emergency.We noted that the Force does not operate a system which allows it to check the equipment that 'belongs' in a vehicle. We reviewed the 'Occupational Driving Policy’ and noted that it is the police officer’s responsibility to ensure that the appropriate equipment is held in the vehicle, which should be checked daily. We noted that there is no auditable trail that can be evidenced to show that equipment checks are being completed.We reviewed a sample of 10 vehicles to ensure that the appropriate equipment was in the vehicle. We used the ‘Vehicle Safety Inspection and Equipment Checklist', and matched this to the relevant department to ensure that the correct equipment is carried on the vehicle. We were not able to inspect four vehicles as the vehicles were out, however for the other six we noted that three vehicles did not have the correct equipment.During our review of equipment management of the Service, we noted that barcodes for equipment are important in ensuring that the correct piece of equipment is checked out to the correct pump on the Redkite system. We identified that for five out of 57 pieces of equipment that was reviewed, there were no barcodes. After discussions with the firefighters, we noted that there is some difficulty in raising a defect in the redkite system if there is no barcode on the equipment.We noted that the full inventory checks of the pump should be carried out on a weekly basis, however we identified that weekly checks had not been noted on Redkite for four pumps and we could not confirm that weekly checks had been completed.*Risk and Impact:* Incorrect equipment may result in a lack of readiness in emergency situations. | The Force should ensure that inventory checks are carried out daily (or as suggested in the policy) and that an auditable trail is kept to evidence that inventory checks are completed.The Service should ensure that all equipment is barcoded where appropriate to allow for effective and efficient inventory checks. | **2** | The organisations will need to implement a new system to support the ongoing management of the equipment within operational fleet. A project mandate shall now be submitted to support the commencement of a new programme of work to implement a new system. The timeline for delivery shall then be determined by the project portfolio capacity, the data cleansing and the procurement process. | Leanne Hanson Chief Asset Officer30 November 2025 |  |
| **2** | **Lack of updated policies and procedures***Observation:* An asset management policy and procedural document allows for resource optimisation, accountability, maintenance planning and ensuring equipment safety.A review of policies, process and guidance documents highlighted that the Service’s Asset Management Guidance document was from March 2020 and did not appear to have been reviewed.Additionally, we were informed by the Head of Transport and Travel and the Chief Asset Officer that there were other policy and procedure documents that were currently out of date, and they are currently in the process of update and review.*Risk and Impact:* The OPCC, Force and Service do not achieve their objectives regarding Fleet / Asset Management and more widely across medium/long term objectives. | The Force and the Service should ensure that policy and procedural documents for Asset Management are updated and shared with the staff members, including the Service’s Asset Management Guidance document. | **3** | The Department is currently undergoing a review and potential restructure. As part of this work is also being undertaken to establish a single Asset Strategy. This shall be aligned to the revised organisational Strategies and Plans. Linked to this will then be a full review of all Policies and Procedures to take into account the revised delivery model | Leanne Hanson Chief Asset Officer30 September 2025 |  |
| **3** | **Lack of equipment testing***Observation:* Equipment testing across the Force and the Service allows for operational readiness to ensure that vehicles and equipment are ready for duty in case of an emergency.We noted at the Force that equipment is 'tested' if required when the police officer does the equipment checks on the car, however we noted that there was no auditable trail for equipment checks therefore cannot confirm that the checks are happening daily as per the guidance in the 'Occupational Driving Policy.*Risk and Impact:* Lack of safe equipment may compromise The Force's ability to respond effectively in the event of an emergency. | The Force should ensure that equipment testing is carried out where appropriate, and include guidance for officers within procedural documents, as well as keeping an audit trail of this | **3** | The organisations will need to implement a new system to support the ongoing management and testing of the equipment within operational fleet. A project mandate shall now be submitted to support the commencement of a new programme of work to implement a new system. The timeline for delivery shall then be determined by the project portfolio capacity, the data cleansing and the procurement process | Leanne Hanson Chief Asset Officer30 November 2025 |  |
| **4** | **Service – Reliance on spreadsheet for the Vehicle Maintenance and Records***Observation:* We noted that Fire Engines (pumps) are serviced every three months, six months and annually. While the Force uses TranMan to track maintenance and availability, the Service currently tracks this using a manual workbook tracked and updated by the Senior Fleet Administrator.We noted that the TranMan Management system is available for NCFRA, but it is not utilised therefore, currently there is no availability tracking system used for fire trucks. Head of Transport and Travel aims to implement the use of TranMan for fire, we noted that this may be a potential area for training.Additionally, we reviewed the sample of recently purchased fire fleet and noted that fire engine services were completed late for three out of eight vehicles. We noted that once the services were completed, they were dated and signed by the brigade technician and the supervising officer*Risk and Impact:* The use of spreadsheets, leads to human error as well as extra workload for operational staff | Once the Service has transitioned to TranMan system, they should implement a programme of training on how to utilise the TranMan system for operational asset management staff. | **3** | The Department is currently undergoing a review and potential restructure. As part of this work the maintenance of the Fire Appliances is being outsourced. Linked to this will then be a full review of all Policies and Procedures to take into account the revised delivery model. And then ensure that the incumbent system is utilised to its full potential whilst work is undertaken to implement a new fleet/equipment management system. | Leanne Hanson, Chief Asset OfficerTheresa Cheney, Head of Transport and Travel28 February 2025 |  |

**Joint Core Financials – 27 November 2024**

|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management Response** | **Timescale/ responsibility** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| **5** | **Credit notes***Observation*: A credit note is usually raised by a service request or email request and approved by a different member of the Finance Operations Team. After approval and once an invoice reference has been entered, the credit note should automatically match to the paid invoice on the system to complete a timely payment.We reviewed a sample of ten credit notes at the Force and NCFRA and noted one instance at the Force where the credit note had failed the automatic matchingprocess, and the credit remain unpaid (£54.79) since April 2024.We were advised by management that this has been raised with the Support Team to who are still investigating the issue.*Risk and Impact:* The Force are unaware of system issues that could lead to further credit note matching issues and delays in payments to customers. | The Force should continue to investigate the issue and seek atimely resolution. Once the issue is identified the Force shouldconsider additional preventative controls, such as systemic controls, that avoid the matching process failure from occurring again | **3** | Credit notes will be completed within the finance operations team. A request will be made via a service request and then entered into Unit 4. Investigations into Unit 4 and automatic matching will continue.Training has been carried out across the team for awarenessUpdate April 2025 - This functionality is now working in most cases, where there is more than one credit this doesn’t quite work like this, but it is fine | Finance Operations Team01 March 2025 |  |

**Workforce Planning – 27 February 2025**

|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management Response** | **Timescale/ responsibility** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **No formal succession plans for critical roles***Observation:* We confirmed an exercise had been undertaken to identify critical roles across police officers and staff. We were provided with a spreadsheet which mapped each role into the following categories:* Tier 1: Core operational function
* Tier 2: Critical support to operational function
* Tier 3: Non-critical support to operational function

However, management advised that formal succession plans had not been put into place for the core or critical roles identified, to ensure establishment stability and continuity of service, manage career pathways, and identify and place high potential staff in leadership roles.*Risk and Impact:* Key roles are not identified, and succession plans are not developed to ensure continuity of service. Therefore, the Force is unable to fill key roles sufficiently quickly, leading to operational deficiency. | The Force should develop formal succession plans for critical roles to establish the dependencies of each role, the role specification, potential successors in emergency, short/medium/long term, and the handover processes should a key member of staff leave at short notice.* Dependencies of each role such as key skills, competencies and qualifications.
* The role specification.
* Individuals with potential to assume critical roles in emergency, short term, medium term or long-term capacity; and,
* Handover processes should a key member of staff leave at short notice.

Succession plans should be periodically reviewed to ensure they are accurate and up to date | **2** | Liaison with Workforce Planning to identify critical roles. Work on going to look at skills for critical roles and how individuals can identify their current skill set and identify any development required. Looking at utilising about me section on Talent Tile of PDR and to utilise the Talent Tile to produce talent pools which indicate when individuals would be ready for role e.g. ready now/short/medium or long term.Update 10/09/25 - Following a meeting with JW, it was acknowledged that the current  critical role list was produced as a result of COVID restrictions. Therefore a questionnaire was produced and sent out to all Heads of departments asking them to review and score roles in their departments to see if they met the threshold for critical roles. Returns were requested by the 17th July and a meeting was held with JW to review the results. A number of departments had not responded so a further chase up was sent out, with nil returns being required too. A follow up meeting has been scheduled for the 24th September. | Caroline Oppido01 September 2025 |  |

**Business Continuity & Emergency Planning Follow Up – 29 May 2025**

|  | **Observation/Risk** | **Original Recommendation** | **Priority** | **Management Response** | **Timescale/ Responsibility** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **Partially Implemented***Observation:* We have reviewed the OPFCC Business Continuity Plan and confirmed that this is now subject to an annual exercise, last performed in November 2024. This recommendation has therefore been considered as Implemented for the OPFCC.We reviewed the Business Continuity exercise schedule for Northamptonshire Force. This states that category 1 departments should be tested on an annual basis. We noted the following however:* The DDAT department was last tested in July 2022: We were advised by the Risk and Business Continuity Manager that they have provisionally got an exercise scheduled for May 2025.
* The Command Team and Executive Support exercise was blank on the exercise management log. We were advised by the Risk and Business
* Continuity Manager that the command team was in a state of transition throughout 2024 due to suspension of the former Chief Constable, so an exercise will be conducted when this team is stabilised.
* The Roads Policing Team exercise was blank within the exercise management log. We were advised by the Risk and Continuity Manager that that this team was introduced in 2023. This should have been tested in 2024 but has not been completed.

We have reviewed the BCP Management Log and BCP Exercise Log and have confirmed that they are consistent with one another.*Risk:* Business continuity plans are not fit for purpose should an incident arise. | **Annual Testing Programme**The Force and OPFCC should implement an internal annual test programme for its business continuity plans.The Force should ensure the test programme covers all plans over a cyclical period, with those of highest priority tested on a more frequent basis.The Force should perform a reconciliation between the BCP Exercise and BCP Management Log, to ensure the departments listed are consistent with one another. | **2** | The DDaT exercise is currently scheduled to be completed by the end of July 2025 but as previously explained it is hoped that this can be aligned with any disaster recovery testing so this date may be subject to change.The Command Team exercise is scheduled to be completed by the end of September 2025.Roads Policing completed an exercise in April 2025Update August 25 – A combined Business Continuity and Disaster Recovery exercise has been approved by senior officers. This will be a force wide exercise which is being developed and will be run later in 2025 when operationally viable. | Force Business Continuity and Risk Manager30 September 2025 |  |

**Procurement and Supply Chain – 18 June 2025**

|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management Response** | **Timescale/ Responsibility** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **Ensuring Contract Award Notices are Published***Observation:* As per the procurement regulations we would expect that notices are published within 30 days of awarding a contract. This should be done through the Find a Tender Service or Contracts Finder.We selected sample of 10 contracts that had various routes to market in the past twelve months. Nine of these contracts would be considered meeting the threshold where a contract award notice would be necessary.We noted six cases where the contract award notice was not on Find a Tender, and instead a decision record was conducted by the PFCC to ensure transparency. We further noted that three of these decision records were not on the OPFCC website. We were advised by management that this can happen where the contract is sensitive.* Furthermore, in the rest of the sample of three contracts, we were not provided evidence of the contract award notice. The force used the EU Supply procurement tender portal at the time.

*Risk and Impact*: The Force is not being transparent regarding contract awards which could result in reputational damage | The Commercial Team should ensure that once a contract has been awarded, there is an appropriate award notice published | **2** | This was a known risk within the department and had been inherited from the transition and dissolution from the outsourced provision. The duplication across systems and double entry of information were not seen to be an appropriate use of limited capacity and mitigations had been established through the publication of decision records and our pipeline to ensure full transparency was provided in an alternative format whilst system reviews and implementation were undertaken. Nevertheless, the action is acknowledged, and steps have already been undertaken as part of the Transforming Public Procurement project to ensure the team are trained on the publication of notices for both PCR 2015 and PA23. In addition, the Organisations have also purchased a single system that shall support the single publication. This is regularly discussed in team meetings and we are monitoring notice publications during the TPP project meetings. An action plan to further monitor compliance is being developed.Update September 2025 - **Complete**- Further training has been delivered to all of the commercial team on the publication of notices on both contracts finder (for some PCR 2015 contracts) and Atamis/Central Digital platform for PA23 contracts. Reminders are made to the team in our stand up calls and notices are monitored through management structures. Notices are being published in accordance with the new regulations and the transitional arrangements under PCR. Example notices can be provided if required | Lucy Westley, Head of Commercial and Business Development01 September 2025 |  |
| **2** | **Conducting a service request when going out to market***Observation:* The May 2023 Joint Code of Corporate and Contract Procedure rules state that contracts over £213,477 must be approved with a service request by the PFCC.We selected a sample of 10 contracts that have had various routes to market in the past twelve months.We noted one contract, Standard Fuel Oils, with a total value of £1,680,000, did not have a service request. We were able to confirm that this contract did have a tender award report which was approved by the PFCC Monitoring Officer*Risk and Impact:* Approvals have not been obtained as per the contract procedures, leading to potential risk inappropriate spend. | The Commercial Team should update the contracts approval process to require a service request for all contracts over the relevant threshold within the Joint Code of Corporate and Contract Procedures prior to approval. | **2** | The Joint Code of Corporate Governance, which includes the Contract Standing Orders shall need to be updated to reflect the commencement of the Procurement Act 2023. Within this the approval levels shall need to be updated accordingly to align to the new requirements laid out in the statutory provision. In preparation for this, the organisations shall seek to establish a procurement panel that will oversee both below and above threshold contracts and the decision process around these. However, it should be noted that It is acknowledged that an SR was not submitted for the one case identified above and this is likely because this award was undertaken via an aggregation exercise with CCS. Therefore, a decision was taken to join the aggregation and the service request not followed up. The agreed route to market was approved via signature summary a month later when the TAR was submitted.Update September 2025 - **Complete-** This action had already been managed as part of the new Corporate Governance Framework publication on 24th February 2025 and the introduction of the new procurement panel process. In addition it should be noted that this process was part of our SOPs prior to this (under old CGF and old regime), but the contract identified was an anomaly | Leanne Hanson, Chief Assets Officer01 July 2025 |  |
| **3** | **Sending timely reminders to suppliers within frameworks***Observation:* The Force manages frameworks for several suppliers. As part of these frameworks, suppliers are expected to send timely management information returns so that the force can charge invoices for the value of work completed. Usually, this management charge is 1%.We selected a sample of four frameworks to assess whether suppliers sent in management returns. Within this sample of four we looked specifically at six suppliers that were part of the frameworks.We noted in one instance where the management information by a supplier had not been sent in accordance with the Estates and Facilities Framework. We were not provided with evidence that Neville Special Projects, a supplier within the Estates and Facilities Framework, has sent in their management returns for at least the past six months.The framework agreement states that that the contractor shall provide information regarding the total amount of charges invoiced by the contractor so a management charge can be calculated. We noted that during audit a reminder was sent to the supplier.*Risk and Impact:* The Force cannot raise invoices in a timely manner due to supplier not sending in management returns. | The Commercial Team should track returns within their totaliser spreadsheets, which are used to monitor framework invoices. | **3** | A further contributory factor to the robustness of this process was the limited capacity within the team. The Business Development team are now back to full establishment, and we have an additional post which has now been approved to support the team. This limitation was already acknowledged, particularly, with the SMEs who are members of the E&F Framework. Processes are being reviewed and re-established to further improve practice. As part of the processes, the compliance of the suppliers to their contractual obligations shall be monitored and reported on within the monthly scorecards provided to the Chief Asset Officer and the Assistant Chief Officer, Enabling Services, to ensure performance management is in place and income secured. However, it is recognised that this is a single supplier out of a large volume.Update September 2025 - **In progress-** Work has been undertaken to improve the tracking and monitoring of framework returns. Since the addition of the extra commercial manager, the staff team for business development have been further reviewed and it is recommended that the administrative support is realigned to help with this area, especially with the introduction of the new IT framework. Significant activity has been undertaken with the E&F framework suppliers to engage and improve returns. A meeting is due to be held on 9th September to forward plan supplier management and income tracking for the next 12-18 months. Revised date 01 October 2025 | Lucy Westley, Head of Commercial and Business Development01 September 2025 |  |

**Joint Governance – 03 July 2025**

|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management Response** | **Timescale/ Responsibility** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **NCFRA – Chief Fire Officer’s expenses not published online***Observation:* The Information Commissioner’s Office (ICO) definition document for joint or combined authorities and boards in part II of schedule I of the Freedom of Information Act1 sets out the kinds of information that the ICO expects authorities, including the fire and rescue authorities and joint or combined authorities, to provide in order to the meet commitments under the model publication scheme.The document states that for members and senior officers the authority should “provide details of the allowances and expenses that can be claimed or incurred” and “include the total of the expenses paid to individual senior staff and authority members”.We reviewed the OPFCC and NCFRA websites and found that the Chief Fire Officer’s expenses are not published online. The Governance and Accountability Manager advised that NCFRA were unaware of the requirements to publish such information.*Risk and Impact*: NCFRA does not follow ICO guidance on publishing Chief Fire Officer expenses and therefore is not entirely transparent, which could lead to reputational concerns. | NCFRA should publish the Chief Fire Officer expenses details online on a regular basis.As part of this, the NCFRA should establish a clear process to enable regular, accurate, and timely publishing of Chief Fire Officer expenses details. | **2** | Arrangements have been put into place that will ensure that with immediate effect the CFO expenses will be published on the Fire and Rescue website on a monthly basis. This is in line with the process followed for PFCC and Chief Constable. This information will be uploaded by Finance team as processed. | Paul Fell - Director of Delivery, OPFCCDon Crook – NFRS31 August 2025 |  |
| **2** | **OPFCC and Force – Policy and procedure review***Observation:*Policies and procedures should act as a key reference for stakeholders to understand what the appropriate procedures are and to ensure compliance with the key regulations that govern the work of the PFCC and associatedparties. Policies and procedures should be reviewed on a regular basis to ensure that they are kept up to date with changes to the legislation that they are built on.We reviewed a sample of 11 policies and procedures covering the OPFCCC, Force and NCFRA and found the following:• The OPFCC Whistleblowing Policy (last reviewed August 2022) and Code of Conduct (last reviewed January 2022) were updated in May 2024 and December 2024 respectively, but neither has been updated on the OPFCC website. Both Policies also do not have a stated review frequency in place.• The OPFCC’s Gift and Hospitality Policy and Procedure was last reviewed January 2022 and due for review January 2023 and so is now out of date.• The OPFCC’s Travel and Subsistence Policy and Equality and Diversity Policy were both last reviewed May 2022 but do not have a stated review frequency.• The OPFCC Record Retention and Disposal Policy was last reviewed May 2022 but does not have a stated review frequency.• The OPFCC FOI Policy was not publicly available as a PDF version and did not have a last reviewed date. The Governance and Accountability Manager advised that the Policy was updated in October 2024 and due to accessibly reasons there is no PDF version online. It is expected to be reviewed annually.• The OPFCC Risk Management Policy was last reviewed March 2023 but does not have a stated review frequency or version control in place.• The Force’s Social Media Policy was last reviewed April 2023 and due for review April 2024 and so is now due for review.*Risk and Impact:* Policies and Procedures at the OPFCC and Force are out of date and may not reflect current practices or changes in legislative requirements, leading to inconsistent operational and strategic activities. | The OPFCC should review all policies and procedures that are past their review date. Once completed, the updated policies and procedures should be published on the OPFCC’s website, in accordance with relevant guidelines, and communicated to all relevant staff.As part of the OPFCC’s review into its policies and procedures, it should ensure all policies and procedures have a clearly stated and documented review frequency in place.The OPFCC should develop and implement a procedure to monitor policies and procedures overdue for review on a periodic basis, such as through a monitoring spreadsheet.The Force should review and update its Social Media Policy. Once completed, the updated Policy should be published on the Force’s website in accordance with its own guidelines. | **3** | SMc pulling a list together re the policies and procedures that require a review and then we can seek to allocate these for review to appropriate staff members. | Jonny Bugg – CEO, OPFCC30 October 2025 |  |
| **3** | **All – External Gifts and Hospitality Registers are not updated or published regularly.***Observation:* We would expect that the Gifts and Hospitality Register is regularly reviewed, updated, and published on the respective websites.OPFCCThe OPFCC Gifts and Hospitality Policy and Procedure (January 2022 – see Recommendation 2 also) states that the Register should be “updated and published as soon as practicable, after the offer has been made.”We reviewed the Register on the OPFCC website but noted that the last entry was dated the 23rd January 2020. We were advised by the Governance and Accountability Manager that internally the Register had been updated but not published online.NCFRANCFRA has its own Gifts and Hospitality Register. This was last published on its website on the 26th June 2024 (with the most recent entry on the Register being dated the 23rd of October 2023). However, upon review of NCFRA’s latest (2024) internal Gifts and Hospitality Register we noted an entry from December 2024. Therefore, the most recent Register has not been published on its website. NCFRA’s Gifts and Hospitality process flowchart does not include a set and clear timeline for the update of the publicly available Register.ForceThe Force also has its own Gifts and Hospitality Register. The Force’s Gifts and Hospitality Policy (June 2024) states that the Register will be published externally on an annual basis. The publicly available Register was last updated the 19th September 2024, with the last entry dated 16th January 2024. However, upon review of the Force’s internal register, we noted that the most recent entry was from April 2025. Whilst the Force is not yet due its annual update (September 2025) of the external Register, the Force may consider implementing a more regular update of its external Register to ensure timely recording and transparency of gift and hospitality information.*Risk and Impact:* The externally published Gifts and Hospitality Registers are not accurate compared to internal versions, leading to transparency issues. | The OPFCC should update the publicly available Gifts and Hospitality Register and regularly ensure it is in line with the internal version. To support this, it should implement a formal and clearly defined timeline, in its Gifts and Hospitality Policy and Procedure, for updating the external Register.NCFRA should update the publicly available Gifts and Hospitality Register and regularly ensure it is in line with the internal version. To support this, it should implement a formal timeline for updating the external Register.The Force should consider implementing a more regular update of its external Register to ensure more timely, accurate, and transparency in externally recorded gift and hospitality information. | **3** | This was completed 4th April 2025 | Paul Fell - Director of Delivery, OPFCCDon Crook – NFRS30 July 2025 |  |

**Police and Fire IT Governance – 29 July 2025**

|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management Response** | **Timescale/ Responsibility** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **Lack of an Organisational Cyber Security Policy***Observation:* Organisations that work in fields such as policing which necessitate a reduced risk tolerance in the realm of cyber security should have a formal cyber security policy. This policy should highlight the additional considerations which must be made to accommodate these enhanced security requirements.The OPFCC, Force and NCFRA utilise the generic “UK Government Cyber Security Policy Framework” in place of a bespoke cyber security policy. This document outlines the basic objectives of cyber security but does not provide either specific standards and requirements for establishing a suitable cyber security presence or contain any reference to the unique requirements (such as enhanced data privacy) inherent to the public safetysector.*Risk and Impact:* The configuration of a cyber security posture around the requirements of a generic cyber security policy can result in the implementation of ineffective cyber security practices and guidelines. This may increase the risk and severity of cyber securityincidents, leading to data breaches and increased vulnerability to hacking and ransomware attacks. | The OPFCC, Force and NCFRA should develop a bespoke cyber security policy document, and related standards/procedures outlining the specific requirements and expectations for its cyber security posture, with consideration for the additional requirements necessary for policing/fire organisations. This document should include an overview of the key controls that should be put in place to achieve the overall objective of the cyber security policy. | **2** | This recommendation is currently being addressed and is effectively monitored through the SyAp framework under Action A1016. The Digital Security Architect is responsible for drafting the policy, with overall accountability assigned to EA.A draft of the Cyber Security Policy is anticipated by early August. While we appreciate the recommendation, we believe the existing framework is already managing this action appropriately.Update from Simon Creasey 01/09/25 - I have prepared the Security strategy to first draft and it is out with my team for review. RC has committed to make sure that I’ll have his feedback when I return from leave on 8th September. I’ll then factor in the feedback and move to publish (as long as no significant changes are required). | Roy CowperEnterprise Architect31 August 2025 |  |
| **2** | **Lack of Consolidated Portfolio Planning***Observation:* Organisations composed of multiple departments should ensure that project resourceallocation is carried out through a unified mechanism across all departments. In addition, whenever possible the development of these projects should be carried outaccording to a unified project development framework to facilitate the inclusion of resources from across the organisation.IT Projects within the OPFCC, Force and NCFRA are often conducted entirely by the police or fire departments without input from DD&T. Where collaboration between departments does occur, each department maintains different ways of working andproject methodologies.While a unified project framework guidance document does exist to align these ways of working, IA were informed by Individuals within DD&T that this is often viewed as too complicated and unwieldy to be regularly utilised and is thus often ignored.*Risk and Impact:*Failure to coordinate project delivery across the entire organisation can result in an unnecessary segregation of resources. This can lead to an inefficient project delivery process due to an underutilisation of skills or a failure to deliver criticalprojects due to an inability to pool resources across teams. | 1. The OPFCC, Force and NCFRA should explore and implement solutions to facilitate the organisation-wide adoption of the Project Framework Guidance methodology.This might include the development of a condensed guidance document to outline the basic principles of the methodology as well as the provision of training to staff across the organisation in the proper implementation of this framework.2. Responsibility over the governance of resources for jointprojects should be delegated to one of the existing jointorganisational committees. | **2** | We accept this recommendation but clarify that it pertains specifically to all digital projects across both organisations and for organisational change projects within Police; as these fall within the DDaT remit and are intrinsically linked to Project Framework.The adoption process is accurately aligned with requirements and monitored effectively within DDaT Transformation and Change. Training and governance are also reinforced through monthly reports submitted to the CDO board and organisational change board; offering detailed guidance on implementation of the framework and providing a clear avenue for escalation of concerns. We will commit to developing formal guidance documentation as well as formallyarticulating the governance framework. | Andrew Jones (Head of Transformation and Change (DD&T)01 October 2025 |  |
| **3** | **Unclear links between governance bodies***Observation:* Organisations that are comprised of multiple semi-independent departments should ensure that the information flows between governance bodies across these departments are mapped both at an organisational level and within the Terms of Reference (ToR) documents for each body.We were informed that no formal documentation has been produced which outlines any connections between the governance bodies of each branch, Police, Fire andDD&T. For this reason, governance bodies which oversee connected topics such as data or service management may fail to inform other bodies of new information or decisions made which may concern them.*Risk and Impact:* A failure to adequately define and account for the connections between governance groups in the OPFCC, Force and NCFRA may result in an unnecessary duplication of work or conflicting decisions. | The OPFCC, Force and NCFRA should formally document andcommunicate any connections that exist in the objectives ordecision-making responsibilities between governance bodiesacross the organisation. This document should be employed toinform DD&T of which boards within the police and firegovernance structures would most benefit from additional direct communication links. | **3** | Both organisations are undertaking a comprehensive evaluation of their governance processes, with a primary focus on improving decision-making through boards, national benchmarks, standardised templates, and enhanced communication procedures.DDaT will commit to evaluating these findings against the existing DDaT governance structure to identify areas for refinement. Identify and map existingconnections and decision-making responsibilities across governance bodies and to draft and review a formal document reflecting these connections | Clare Chambers (Chief Digital Officer)31 December 2025 |  |
| **4** | **Data Quality Assurance Procedure***Observation:* Organisations that frequently deal with large quantities of data should develop a data quality policy to ensure that data is accurate, organised and readily available to relevant stakeholders. A data quality policy should include controls such as regulardata reviews or the creation of data input templates that guide the data input and processing activities of employees.We were informed that no data quality policy has been put in place to influence the DD&T balanced scorecard reporting mechanism, with the only data quality process currently taking place being manual data validation by the heads of each DD&T process.*Risk and Impact:*A failure to implement a data quality policy may lead to the creation and processing of incomplete or inaccurate data. Judgements made usingthis data may fail to address the actual issues impacting performance within DD&T. | The OPFCC, Force and NCFRA should create and implement adata quality policy, detailing the organisation’s requirements fordata input, storage and analysis. | **3** | The Head of Information Assurance and the Head of Performance and Business Insights have collaborated to develop a draft Data Strategy. This strategy integrates key elements of data quality, including input, storage, and analysis, into a cohesive framework. Scheduled for presentation at the June CDO board, the strategy will undergo wider approval before being followed by tailored implementation plans designed to address specific service requirements. | Trina Knightley-Jones (Head of InformationAssurance)01 August 2025 |  |

**Joint Estates Management – 22 August 2025**

|  | **Observation/Risk** | **Recommendation** | **Priority** | **Management Response** | **Timescale/ Responsibility** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| **1** | **Completion of stock condition surveys***Observation:* A stock condition survey is a detailed visual inspection of a property, whereby a qualified surveyor assesses the age and condition of a building to help identify potential hazards and inform repair and maintenance programmes.The Force and NCFRA outsource completion of their condition surveys to Gleeds. Whilst there isn’t a legal requirement for the Force and NCFRA to have surveyscompleted regularly, we noted through discussions with the Joint Property Operations Manager that they aim to have them completed every five years, which is in line with best practice across the sector.We selected a sample of 10 properties, five from the Force’s estate and five from NCFRA’s, and sought to confirm a stock condition survey was completed within the last five years. We noted the following exceptions:* Two properties had not had a stock condition survey completed (St James Box from the Force’s estate and Chelveston Training Station from NCFRA’s estate).
* Two properties had a stock condition survey completed over five years ago (Daventry Police Station and Force HQ – HR Block both from the Force’s estate had surveys last completed in 2018).

*Risk and Impact:* The absence of regular stock condition surveys hinders both the Force and NCFRA’s ability to maintain accurate oversight of the condition of their estate, therefore impacting maintenance programmes as issues are not identified in a timely manner. | The Force and NCFRA should engage a provider toconduct stock condition surveys for all outstandingproperties as soon as possible where one hasn’t beenconducted within the last 5 years, including propertiesoccupied within the last 5 years.2. The Force and NCFRA should introduce a centralisedregister recording all buildings within their estate and thedate the most recent stock condition survey wascompleted.3. A control should be introduced to allow for the timelyidentification for buildings that are due a stock conditionsurvey after five years. | **2** | 1. The Force and NCFRA shall assess the most suitable provider, subject to compliance with Procurement Act 2023, to undertake a conditions survey programme for all outstanding properties within the identified perimeters. The prioritisation of these shall be aligned to the Estates Strategy, once agreed and finalised.
2. The Force and NCFRA shall seek to create an interim measure for this, as the delivery of a software solution is currently being aligned across the organisational priorities.
3. As set out in 1&2 above the control to identify shall be aligned and implemented on an interim measure whilst a software solution is awaited.
 | Leanne Hanson, Chief Asset Officer30 January 2026 |  |