THE POLICE, FIRE AND CRIME COMMISSIONER OF STAFFORDSHIRE AND THE CHIEF CONSTABLE OF STAFFORDSHIRE

Asset Management – Asset Tracking (Advisory)

Final Internal audit report: 2.20/21

4 December 2020

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

1. EXECUTIVE SUMMARY

With the use of secure portals for the transfer of information, and through electronic communication means, remote working has meant that we have been able to complete our audit. It is these exceptional circumstances which mean that 100 per cent of our audit has been conducted remotely.

Background

An advisory review of Asset Management – Asset Tracking was undertaken at the Police, Fire and Crime Commissioner of Staffordshire and the Chief Constable of Staffordshire (the Force) as part of the approved internal audit periodic plan for 2020/21.

The Force currently has around 3,500 staff members employed which includes approximately 1,700 Police Officers. As a result, the Force maintains a large and wide variety of assets and it is therefore fundamental that these assets are appropriately safeguarded and well managed.

Prior to December 2019, the Force's asset management processes, in relation to IT Hardware and Software, were being managed by Boeing. The contract with Boeing terminated in December 2019 following a four-year partnership. A dedicated IT Department was therefore brought back in-house in July 2020, which currently has around 70 staff members. Forty of the 70 staff members were TUPE'd from Boeing and an additional 30 new staff members were recently recruited by the Force.

A project was initiated towards the start of the current financial year which focused on the physical and digital assets currently managed across the Force. The project is being overseen by the Head of Corporate Planning and Business Change and Project Support Officer. At the time of review, the Force was at the stage of commissioning a formal project scope, which is due to be completed following the issue of this report.

Asset management is broadly defined as the proper safeguarding and recording of assets. The key elements of a good asset management framework are as follows:

- The maintenance of accurate records via an asset register or inventory log;
- Awareness of the physical location of assets;
- Allocated custodians for individual assets; and
- Periodic and systematic physical verification of the existence and condition of assets to protect against theft, fraud, and detect the unauthorised use of property.

As part of the initial planning process, the Force completed an exercise to broadly ascertain the current assets in place across the Force and group them accordingly. Following this exercise, a proposed draft project scope was developed based on the following five high priority areas:

1) Software and IT Hardware;
2) Police Equipment Issued to Persons;
3) Police Vehicles;
4) Evidential Data Assets; and
5) Non-Evidential Data Assets.

In addition to the above five areas, the Force has considered key departments and partnerships which provide a vital role in the asset management process such as the Fire and Rescue Service (FARS), Estates and Support Services, Information Governance, HR, and IT Departments etc.

As part of this review, we have focused on areas 1) Software and IT Hardware, 2) Police Equipment Issued to Persons and 4) Evidential Data Assets. Discussions have been undertaken with key staff members across various departments covering the above three areas to ascertain what assets they manage, and to evaluate the current asset management processes they have in place.

Observations – wider sector experience

Some forces use the following asset management systems;

- Hardhat

- SAP

- Real Asset Management

- Miquest

But these systems alone do not necessarily provide a full solution for all asset management. They are often not capable of recording or tracking all asset types – for example firearms, where separate systems or spreadsheets are held. Clearly, they do reduce the number of individual systems and spreadsheets held, but do not always provide that full solution.

An organisation needs to understand fully from the outset the assets that they have, where they are, replacements etc. before any system is then implemented and rolled out. The core data needs to be data cleansed and therefore accurately reflected in the spreadsheets and systems that are already in place before migrated onto any system. Stocktaking ahead of any transition/migration is also recommended for high value areas. It is important and this is a reflection of the good practice that we see across other forces and indeed other sectors (where they have also recognised weaknesses in their asset management controls), is to have a solid governance framework in place – others have clearly defined asset management policies supported by clear procedures which ensures the correct allocation of assets to either individuals or departments. This is underpinned by an overall governance framework that includes defined processes and controls for new asset authorisation, disposal, asset tracking and monitoring and even performance reporting against KPI's.

Other forces have developed business flow processes to identify, approve and allocate new assets, based on requirements and replacements.

Conclusion

This review was an advisory audit and as a result, no formal assurance opinion has been provided.

The Force were aware that asset management was a particular area where accountability and improved oversight was required / needed to be strengthened. As such our audit has focused specifically on a few key areas and has provided the Force and the Commissioner with a roadmap to make improvements and to incorporate actions within the internal project.

Ultimately, the Asset Management Framework and Asset Register should be supported by a defined governance framework to ensure the Force and Commissioner are clear what assets they own and their location(s). In addition, we have identified a number of key elements which should be adopted and incorporated within the internal project group. Furthermore, a number of areas have been highlighted which will improve the efficacy of the detail recorded within any supporting Asset Management Framework and also areas where supporting evidence should be linked and / or improved to provide robust supporting registers.

It is acknowledged that given the volume and type of assets involved, that one single Asset Register will not be the most appropriate solution and to make the use of existing systems or spreadsheets (particularly where there are specific nuances) is an appropriate way forward. However, an Asset Management framework should be in place that provides that overarching linkage to the separate asset registers in place across the organisations. The overarching register could include hyperlinks or system links to the location of those departmental registers. As with any process or system, it is fundamental that the data recorded is accurate and that there are routine checks in place to validate and substantiate the data that is included in the asset registers. This needs to become routine practice and across the wider public sector there are requirements for oversight and assurance to boards and committees that there is an up to date Asset Register in place and this may also be something to consider introducing.

We have included a total of 2 high, 11 medium and 7 low priority management actions to assist the Force with a roadmap to make improvements in this area and inform the internal project. There are however some areas that do require immediate attention.

2. DETAILED FINDINGS AND ACTIONS

General

Asset Management Policy and Procedures

The Force does not currently have an Asset Management Policy or accompanying procedures in place.

Best practice dictates that the Force should develop an Asset Management Policy which details overarching guidelines, practices and governance arrangements for asset management across the Organisation. Additionally, as the majority of the Force's assets are managed at a departmental level, it is recommended that each department creates procedures to supplement the overarching Asset Management Policy and clearly detail the management process for the relevant assets within their remit.

Management Action 1	
The Force will develop an Asset Management Policy and disseminate the Policy to all relevant staff members. Additionally, departmental procedure notes will be developed to accompany and support the implementation of the Policy, which incorporates operational practices for the safeguarding and maintenance of assets.	**Priority - Medium**

Asset Registers

The Force does not currently have an overarching Asset Register in place.

Individual departments maintain their own registers based on upon the assets which they manage. Some departments have dedicated systems in place for the tracking and management of assets, and others have adopted manual approaches such as spreadsheets. Actions have been raised throughout this report to address instances where a departmental register was not found to be in place, and if a register was located it was found to be incomplete or not fit for purpose.

Physical Verification Exercises

As individual departments across the Force maintain their own asset registers, they are also responsible for conducting periodic physical verification exercises to ensure those records contained within the registers continue to be accurate. Additionally, physical verification exercises allow departments to confirm that assets remain in a satisfactory condition and are still effective for their intended use. Actions have been raised throughout this report where departmental verification exercises have not been completed or completed on a timely basis.

IT Hardware

Asset Register

Boeing was previously managing the Force's IT hardware and software assets via the Snow Asset Management System, and following the contract termination, a CSV Excel file extract from the System was provided to the Force. However, through discussion with the Chief Technology Officer, we were informed that the file extract was out of date and not a clear representation of the current IT assets which had been distributed across the Force. The Force does not have any additional asset logs in place, and therefore it is imperative that the Force begin the compilation of a dedicated Asset Register for the logging of IT hardware assets.

Management Action 2	
An Asset Register will be compiled and maintained by the IT Department for the logging and tracking of all IT hardware assets across the Force.	**Priority - High**

Mobile Devices

A dedicated system (AirWatch) is in place for the management of all the Force's Samsung Note-9 mobile devices. The Force has recently completed a refresh programme of their mobile devices which resulted in the disposal of all previous mobiles and the procurement of 1,500 new devices (the audit did not confirm that all previous mobiles had been appropriately disposed). The AirWatch System allows the IT Department to allocate specific devices to Force staff members based on their unique collar number and the devices serial number. The all-in-one platform contains functionality for the allocation, monitoring, disabling and reallocation of mobile devices. As of current, the AirWatch System allows for robust management of all mobile devices and it is therefore the intention of the Force to maintain this current System going forward.

Personal Radios

A dedicated system (Airwave Solutions) is in place for the management of all the Force's personal radio devices. All radio devices are personally issued based on the device serial number and relevant staff members collar number. The Airwave System contains functionality for the allocation, monitoring, disabling and reallocation of radio devices. As the Airwave System is the dedicated radio platform in use across the emergency services within the UK, the System will be maintained by the Force going forward.

Laptops

At the start of the Covid-19 Pandemic, the Force was tasked with assessing their current position in regard to providing remote working provisions for relevant staff members. The IT Department confirmed the Force had around 450 laptops in circulation which would be sufficient based on the number of staff members who would be working remotely. The initial number of laptops was determined based on the information provided by Boeing as part of the handover process, however it soon became apparent that the number may not be accurate due to the asset management system not being kept to up to date. The list was found to contain retired members of staff and the Force had to commission a small project team to ascertain the whereabouts of each documented laptop.

The IT Department now have the functionality to monitor laptop usage such as when they were last used and where. However, it was noted that there is not a clear allocation and return process for laptops, with departments often maintaining them when not required, on the off chance that they may be required at a future date. Additionally, although the laptops are heavily encrypted and the IT Department can monitor usage via login credentials, they are not personally issued and as a result they often change hands within the Force based on needs and requirements without the IT Department being notified.

The current laptops in use are running on the Microsoft 7 Operating System and it is therefore difficult for the IT Department to procure additional laptops as the operating system has now been discontinued. The Force is now in the process of procuring new laptops to replace existing stock which will run the Windows 10 Operating System and Office 365 via the National Enabling Programmes (NEP). The Force is intending to procure around 1,500 new laptops by the end of the current financial year and is currently part way through the tender process which is being led by the Commercial Department.

Following the procurement of the new laptops, it is imperative that the Force ensure access to the previous laptops has been fully disabled and the hardware has been collected and disposed of. The Force will then be in a strong position as they can incorporate the issuing of the new laptops within the revised asset management process. The Force also need to ensure that laptops are appropriately tagged, issued and monitored via an effective Asset Register. Clear procedures need to be developed and implemented across the Force to specify the processes around the requesting, issuing, returning and transferring of laptops across the Force. We would recommend that the IT Department frequently monitor the use of laptops to ensure they are being regularly used and only used by intended staff members. Where the system highlights that a laptop has not been used for a prolonged period of time, the Force should ensure that a request is made for it to be returned to IT for storage or reallocation.

Management Action 3	
Following the procurement of new laptops, the IT Department will ensure that all previous laptops in circulation have been fully collected, disabled and disposed of.	**Priority - Medium**

Management Action 4	
Following the procurement of new laptops, the IT Department will ensure that all devices are tagged, logged and monitored on an Asset Register.	**Priority - Medium**

Management Action 5	
Procedures will be developed to classify the processes regarding requesting, issuing, returning and transferring of laptops across the Force.	**Priority - Medium**

Body-Worn Video

The Force currently has around 1,700 body-worn cameras within their inventory. The cameras are currently managed by the IT Department and issued upon request. Tracking of the issuing and returning of cameras is managed via a spreadsheet which documents the individual a specific camera has been allocated to, based on their Force collar number. Through discussion with the Force Incident Manager, we confirmed that as the cameras are issued upon request and there is no clear process of managing returns, instances have arisen where staff members have held on to the cameras longer than necessary.

Firstly, the Force needs to determine which staff members require or may require access to a body-worn camera as part of their day-to-day duties. A management action has not been agreed on this point as it has been covered further on in this report as part of the new starter process and equipment mapping exercise.

Following this, the IT department need to consider personally issuing cameras for staff members requiring frequent use and holding the remaining stock in inventory for issuing when required. Where a camera has been issued on a temporary basis, a clear procedure needs to be in place for the return of the camera to the IT Department when no longer required (eg when moving roles), this will ensure that they remain available for other staff members when required.

Management Action 6	
The Force will review the current process regarding the issuing of body-worn cameras and consider personally issuing cameras to those staff members who require frequent access to one. A clear procedure will be implemented for the returning of cameras to the IT Department when staff no longer require them as part of their duties.	**Priority - Medium**

Additionally, the Force need to consider tracking the issue of body-worn cameras via the NICHE System as opposed to a manual spreadsheet. The NICHE System has an integrated records management module which can be used for issuing physical assets. The unique serial number for each camera can be logged on the System and allocated to a specific staff member based on their Force collar number. All cameras can be input into the system and allocated as well as reallocated when required.

Management Action 7	
The Force will consider tracking the issuance of body-worn cameras via the NICHE System.	**Priority - Low**

IT Software

Asset Register – Software and Licenses

Following the procurement of new laptops, the IT Department will have to evaluate the capabilities of current software in use and ensure they are compatible with the Windows 10 Operating System. This again will provide a good opportunity for the Force to review the current software in place, ensure all software packages installed are being used, review the number of licenses in place and if they are sufficient, as well as ensuring the final position in regard to software and licenses is logged and maintained within an Asset Register.

IT software assets including installations, user access and licence procurement and allocation were previously managed by Boeing via the Snow Asset Management System. The IT Department now has a Contract Register in place which documents software assets and licenses, however we were informed that the Register may not be fully up to date and requires review. Therefore, we have agreed a management action for the IT Department to incorporate a dedicated software Asset Register, which fully details all software currently in use, number of licenses (if applicable) and installation locations.

Software updates are currently delivered to laptops both physically and remotely. We understand it is the intention of the Force going forward is to have a network in place which will allow all software updates, upgrades and patches to be delivered to laptops remotely. At the time of audit, certain software modifications would require the IT Department to physically have custody of the laptops to deploy them, this provides an additional strain on resources across the Department and further complicates the asset management process.

Management Action 8	
The IT Department will ensure all software currently in use, the number of licenses and installation locations are logged on a dedicated asset register.	Priority - Medium

Management Action 9	
Following the laptop refresh across the Force, the IT Department will ensure mechanisms are in place which allow all software updates, upgrades and patches to be deployed remotely.	Priority - Medium

Starters, Leavers and Transfer of Roles

We held a discussion with key staff members within the HR and IT Department to discuss and review the current processes in place regarding the management of assets as part of the Force's starters, leavers and transfer process. The HR Department currently uses the Origin Resource Management System which has been designed by Capita to specifically meet the HR needs of forces across the UK.

Starters

Following the appointment of a new staff member, notifications are issued to relevant departments by HR to allow them to begin processing the new starter. The IT and Payroll Department receive an automated notification via the Origin System and a manual notification is used to the Stores Department. Although the HR Department is involved in the general recruitment procedure, responsibility of the issuance of equipment and assets sit with the other departments across the Force. The Stores Department are responsible for the issuing of uniforms and the IT Department are responsible for issuing general hardware equipment such as mobile phones, radios and laptops.

Through discussion with the IT Department we confirmed that a standardised procedure is not currently in place for the issuing of equipment to new starters within the Force. As a starting point, we have agreed a management action that the IT Department, in conjunction with other key departments, compile a list of necessary equipment for each role within the Force. This exercise of mapping equipment to specific roles will help to ensure that individuals have the correct kit and equipment upon commencing employment and will reduce the risk of staff being allocated unnecessary equipment which they do not require as part of their day-to-day duties. Additionally, the mapping exercise should incorporate the use of systems across devices such as laptops and mobiles to ensure relevant software has been installed and access appropriate rights granted.

Following this initial mapping exercise, the IT Department should implement a new starter checklist which can be used for each new starter to ensure all required equipment has been issued in a timely manner post appointment.

Management Action 10	
A mapping exercise will be completed to determine what initial equipment (hardware and software) is required for all roles within the Force.	**Priority - Low**

Management Action 11	
A new starter checklist will be introduced by the IT Department to ensure that all necessary equipment has been issued to new starters in a timely manner.	**Priority - Low**

Leavers

Similarly to the new starter process, the IT and Payroll Department receive an automated notification via the Origins System, around one month prior to the individuals leaving date, informing them of a leaver.

A manual notification is issued by the HR Department to the Stores Department informing them of the leaver.

The HR Department has a leavers checklist in place for the management of all leavers and ensure that relevant procedure has been followed, such as actioning the HR System and conducting exit interviews. However, the HR Checklist does not account for the returning of Force issued equipment. Currently, the leavers relevant Supervisor is responsible for ensuing issued equipment has been returned prior to the staff member leaving the Force.

Through the discussion with the IT Department, we confirmed that a formal process is not currently in place to monitor the returning of equipment for leavers. This is a basic control and the IT Department need to implement a leavers checklist which will be completed for all leavers to ensure that all equipment within the IT Departments custody such as mobile phones, radios and laptops have been returned. The leavers checklist should incorporate the disabling of systems access as well as the disabling and returning ID access badges which allow physical access to the Force's buildings.

Management Action 12	
A leavers checklist will be implemented by the IT Department to ensure that all necessary equipment has been returned prior to a leaver exiting the Force. The checklist will account for all issued physical hardware, access disabling on systems and the return of ID badges.	**Priority - High**

Transfer of Roles

Through discussions with key staff members within the Force, we confirmed that it is common for staff members to frequently change roles within the Force and vary their day-to-day responsibilities. Upon a staff member adopting a new role it may not be necessary for them to have access to their current issued hardware or software, and in some instances, they may also require new and additional equipment. It is therefore important that the IT Department complete the mapping exercise discussed above, so that in the event that a staff member adopts a new role, the Department can easily determine what equipment can be returned, and if required, what new equipment to issue.

When a staff member is due to move roles, the HR Department currently complete a 'Moving Sheet' which is issued to all relevant key departments such as IT, Finance and Payroll etc.

In order to ensure that all equipment is being returned and software access is being disabled where necessary upon a staff member moving roles, it is recommended that the IT Department implement a transfer of role checklist. This would also have the added benefit that software licenses can be reallocated to other staff members who require them.

Staff members transferring to another Force are required to return all issued equipment and will be processed through the leaver procedure detailed above.

Management Action 13	
A transfer of roles checklist will be introduced by the IT Department. The checklist will be completed for all staff members transferring roles to ensure they only have the required equipment and access to systems necessary for their new role.	**Priority - Low**

Additionally, the event may arise where a staff member has not formally changed roles but may require access to additional hardware or software as part of their existing role. In such instances, a formal process should be introduced whereby a request is made to the IT Department (following appropriate approval), possibly via the Hornbill IT Service Desk. This process will ensure that additional equipment or software access outside of their determined role requirements, is only issued where necessary.

Management Action 14	
The IT Department will develop a procedure for staff members to request additional hardware or software access.	Priority - Low

Stores – Uniform

Uniform for the Force is stored, allocated and managed by the FARS Stores Department. The Stores Department is located at the FARS Headquarters and is currently managed by seven staff members. Stock is tracked and managed via the Integra Stock Management System which contains an audit function to allow a report to be generated of all stock issued.

Uniform items that are currently stocked for Force staff members include:

- Clothing;

- Custodian Helmets;

- Gloves;

- Handcuffs;

- Batons; and

- First Aid Pouches etc.

All uniform is personally issued and tagged upon issue based on the staff member's collar number. The Supplies Manager completes a rolling annual stock take of all uniform which is split between Force and Fire stock. Supporting documentation for the stock take is provided the Force's Finance Department towards the end of the financial year. Force uniform stock at the end of the 2019/20 financial year was valued at £310k.

New Starters

When a new Officer commences employment with the Force, a notification is sent to the Stores Department by the Force's HR Department. The relevant individual will arrange an appointment with the Stores Department to get measured and fitted and collect their uniform around a week prior to their start date.

Through discussion with the Supplier Manager, we were advised that notifications are received in a timely manner in relation to new starters and sufficient time is allowed for them to collect required uniform prior to their official start date.

Leavers

When an Officer terminates employment with the Force, a notification is sent to the Stores Department by the Force's HR Department. The relevant leaver is supposed to return their uniform to the Stores Department, at which point they will be issued with a certificate confirming return of their uniform.

However, through discussion with the Supplies Manager, we were informed that notifications are not always received, and in many instances the relevant leaver will contact the Stores Department to inform them they are leaving the Force, and ask what they should do with their uniform. In many cases the relevant leaver will give their uniform to their Supervisor or another colleague to return to Stores for disposal. It is recommended that a process is implemented to ensure that notification of all leavers is sent to the Stores Department in a timely manner. Following notification, the Stores Department can cross reference each leaver to ensure that they have returned their uniform and that a certificate has been issued confirming the return.

Management Action 15	
The Force will undertake a review of the current leavers process in regard to the returning of uniform. A revised procedure will be implemented to ensure that timely notification of all leavers is sent to the Stores Department by the HR Department. All notifications will be maintained on file by the Stores Department until the relevant individual has returned their uniform and a corresponding certificate has been issued.	Priority - Medium

Tactical Planning Unit

The Tactical Planning Unit specialises in providing the Force support, resilience capability, contingency and operational planning assistance.

Personal Protective Equipment (PPE) and Chemical, Bacteriological, Radiological, or Nuclear (CBRN) Suits

The Tactical Planning Unit manages various PPE and CBRN suits. The assets are held in a secure store at Watling Street Police Station and currently only tracked for insurance purposes. As of current, all CBRN suits are personally issued to CBRN responders and retrieved from storage as and when required. The Force is currently in the process of refreshing PPE and CBRN equipment.

Management Action 16	
Following the refresh of PPE and CBRN equipment, we will implement a process for the tracking of the assets. The process will include physical verifications and condition checks to confirm the effectiveness of the suits.	Priority - Medium

<u>Drones</u>

Two drones are currently in place which are managed by the Unit and a further drone is currently in the process of being procured by the Force. The drones are stored in a secure storage unit at the Staffordshire Police Headquarters and can only be checked out by 12 dedicated pilots for specific jobs (where usage is appropriate and sufficient approval is in place). The drones are currently managed and tracked via a manual spreadsheet. We consider that the current measures in place are appropriate as the drones are not frequently used and are returned to storage following each job. In the event that one of the drones could not be located, the Unit could easily determine when it was last checked out, for what job and by which pilot.

After each job, footage from the drone is downloaded on to a local shared drive and appropriately tagged. If the footage is in relation to evidential data, the video is tagged and retained until investigations have concluded. If the footage has been obtained for non-evidential purposes, the video is stored on the shared drive and deleted after a period of 31 days.

<u>Medical Kits and Miscellaneous Assets</u>

The Unit maintains an array of public order medical kits which are stored at the Staffordshire Police Headquarters. Some kits have been allocated to specific medics within the Force and some are held in storage until they are required. Additionally, the Force holds scene tents, generators, public order shields, torches and lights etc. These items are currently tracked via a spreadsheet (TPU Kit Asset Register), however at the time of review the spreadsheet had not been maintained and therefore it was not up to date. No checks are currently undertaken in regard to stock levels and the spreadsheet is not updated to record when assets are issued, reissued or returned. The Unit therefore need to implement a more robust method of managing their assets to ensure they are aware of stock levels, physical location and condition.

Management Action 17	
Medical kits and miscellaneous assets managed by the Tactical Planning Unit should be appropriately tagged and managed to account for the issue, return and reissue of items. A physical verification exercise should be introduced to ensure that stock levels as per the asset register are accurate and that items are still in a satisfactory and usable condition.	**Priority - Medium**

Force Armoury

<u>Firearms and Tasers</u>

The Force's Armoury is located at the Staffordshire Police Headquarters which stores the Force's weaponry stock. Some stock is also held at various outstations.

Weaponry in use across the Force including tasers, firearms and ammunition are currently managed via the Chronicle System. Individual staff members are logged on the System based on their collar number. Further supporting information is added to each user such as their qualifications, training, licenses (including validity periods) and any specialist roles that they hold. Through this additional information the System can determine which assets that staff members should be allowed access based on pre-determined parameters. Specialist Force Armoury staff members are able to add, amend and block access as appropriate. Each user on the system is allocated a personal issued ID card which is scanned to allow access.

All tasers, firearms, ammunition details etc that are stored within the Chronicle System have been tagged with a unique identification RFD number. Items are allocated from the armoury based on individual collar numbers, and therefore the Force is able to confirm, at all times, what assets are currently in use and which staff members they have been issued to. Additionally, a stock list audit report can be produced at any point from the System which can confirm stock numbers and the number of items which are in storage and the number of items which have been issued.

Taser safes are in place which store the Force's taser stock. The safes are linked via a network to the Chronicle System and allow tasers to be issued and returned by staff members based on individual allocated access rights within the System. Backup keys for the safes are located in a box safe at the relevant safe locations which are monitored and used if necessary, by an on-site Supervisor.

Although a dedicated system is in place for the tracking and monitoring of the Force's weaponry, there is no process currently to confirm if the stock levels recorded within the system are accurate. We would recommend that periodic physical verification exercises are completed alongside spot-check exercises of the armoury and safes to confirm the assets in circulation are accurately reflected within the Chronicle System.

Management Action 18	
A process will be implemented to periodically physically verify the stock records held within the Chronicle System to the Force's Armoury and safes.	**Priority - Medium**

PAVA Sprays

PAVA incapacitant sprays spray cans are held in the Force's Armoury and are allocated, tracked and managed via the Inca System. All Officers should have an allocated PAVA spray can as part of their personal kit. Each PAVA can has a unique serial number which can be linked to a staff members collar number. Canisters can be tracked on the System at any time, whether they are in storage, transit or with an officer. A warning facility for canister expiry is built into the System to ensure staff members will always have safe and functional canisters in operation. When a PAVA can has been used or has expired, the can is returned for destruction and a corresponding certificate is issue.

There are various issues with the use of the Inca System across the Force. Firstly, a project was recently completed towards the beginning of the current financial year to review the data within the System and confirm its validity. Through discussion with staff members involved within the project, we were advised that the System contains outdated information which was not reflective of the current position across the Force. We were also advised that sufficient training has not been provided to relevant staff members regarding the use of the System, and therefore it has not been regularly updated when cans spray cans have been allocated, returned, expired and destroyed.

Due to the technical nature of the Inca System and the lack of validity for the data contained within it, w would recommended that the Force retire the System and consider an alternative System. Initially, the Force needs to complete a data cleanse of the information pulled from the Inca System and ensure they have a current and up to date record of all cans in inventory, circulation (and to which officers they have been allocated) and corresponding expiry dates.

As the Inca System does not currently offer any advanced asset management or tracking functionality, it could be argued the management of PAVA spray cans does not warrant the use of its own dedicated system. Therefore, it is possible that PAVA cans could be managed via the existing NICHE System. The NICHE System has an integrated record management module which could be used for logging all PAVA cans and allocating them to staff members via their unique collar numbers. The Force should also ensure that the expiry date for each spray can has been logged alongside its serial number, which will allow the Force to ensure that all cans in issue are still valid and recall any expired cans.

Management Action 19	
A data cleansing exercise will be completed of the data held within the Inca System in regard to PAVA spray cans to ensure it is reflective of the Force's current position and is up to date. The Force will then consider retiring the current Inca System and migrating the data to the NICHE System.	**Priority - Low**

Working at Heights and Protest Removal Department

The Working at Heights and Protest Removal Department currently comprises of 14 Officers. The Department is dual purpose and manages assets that are required for Officers to carry out works from heights and on-the-ground protest removal. All equipment is currently stored within a large on-site storage vehicle at the Staffordshire Police Headquarters.

Working at Heights Assets

The Department currently manages 14 climbing harnesses and accompanying kit including gloves, helmets, goggles and ropes etc. All 14 harnesses have been personal issued to staff members within the Department and name tagged. Two additional spare kits are also in place which are often used by the Negotiations Team.

We were advised the harnesses and accompanying kits are not logged on a register or inventory list. Due to the nature of the assets, they only have a limited shelf life based on manufacturer guidance and should therefore be inspected at regular intervals to ensure the kit remains in satisfactory condition and will be effective for their required use.

Protest Removal Assets

The department maintains an array of various manual hand and power tools to aid in protest removals when required. The power tools have been recently acquired subsequent to a training session delivered by the MET Police and hold an approximate value of £5k. A generator is also stored on the storage van for tool charging purposes.

The protest removal assets are not currently tagged and are not logged on a register or inventory list.

It is recommended that the Department complete a tagging exercise for all tools in the inventory which are managed by the Working at Heights and Protest Removal Department. Certain tools, for example power tools will have unique serial numbers which can be used for tagging purposes.. This information should then be recorded in a central location such as an Asset Register for tracking and management. As tools are currently removed from storage by staff members in the Department when they are required and returned back when no longer needed, there is no tracking mechanism in place. Therefore, on completion of the Asset Register, a process should be introduced whereby all tools are allocated and booked out to specific staff members based on their collar numbers. Physical verification exercises should also be completed to cross reference the register to physical stock holding and to confirm the condition of tools.

There may be a future possibility to manage the Department's assets through a dedicated or existing system within the Force, for example the NICHE System. However, the initial required process for the Department is to create a centralised register of all assets in their custody, possibly via a spreadsheet, and ensure they are all trackable via a unique identifier. After this exercise has been completed, the Department can consider migrating the data to a system for allocation, returning and reallocation management.

Management Action 20	
The Working at Heights and Protest Removal Department will consider producing an Asset Register for the logging of all assets that they manage. All assets will be tagged, and corresponding information documented such as where they have been personally issued. Where assets have not been personally issued, a log will be maintained of when items have been issued and returned. Furthermore, a procedure will be created for periodic physical verification exercises that review stock levels and the condition of assets.	**Priority - Low**

Evidential Property and Data Assets

Seized Physical Property

We were advised that seized evidential property such as cash, firearms and drugs etc are currently deposited across stores in the Hanley, Cannock and Burton Police Stations. The Force is intending to store all property at a single location (Watling Street Police Station) going forward.

All evidential property is appropriately tagged and managed through a built-in property management module within the NICHE System. Officers are able to book property in and out of storage via the NICHE System which is logged based on their unique collar number.

Body-Worn Cameras

The Force currently uses Axon body-worn cameras which upload all captured data to the evidence.com server. Staff members are able to connect their camera via a docking station and review captured footage on the dedicated website. Due to the functionality restrictions in place by the camera manufacturer, it is not possible for the Force to store captured data footage locally.

Paper Files and Photographs

The NICHE System has functionality in place for the scanning and storage of paper files and photographs taken by staff members. The System cannot currently store video files; however, a dedicated storage system (ELF) is in place for the storage of general recorded video. Video recordings from the use of drones are stored on a local shared drive with restricted access, and we were informed that data is maintained in line with set retention periods based on their evidential use.

Finance and Procurement

The Finance Department has a dedicated Accounting Asset Register in place which is managed by the Chief Accountant. All capital expenditure including land and buildings are recorded within the Register. Invoices are matched to assets when they are received and paid by the Department.

The Force's current procedure means that all capital expenditure in excess of £10k is capitalised and documented within the Register. Assets related to equipment are depreciated over a 10-year life span and vehicles are depreciated over a five-year life span.

Depending on the asset in question, disposals are either sold online, auctioned or scrapped depending on their functionality, condition and market value.

Procurement is managed by the Force's Commercial Department. The Force does not currently have set refresh periods in place for assets and they are replaced as required and when a strong business case can be made to support the refresh. High-level expenditure in relation to asset purchases are approved by the Commissioner, prior to an appropriate tendering exercise being completed by the Department.

APPENDIX A: SCOPE

Scope of the review

The scope was planned to provide assurance on the controls and mitigations in place relating to the following risks:

Objective of the risk under review	Risks relevant to the scope of the review	Risk source
Modern Policing	Linked to OPCC Strategic Risk Objectives:	Corporate Risk Register
There are adequate controls over the management of assets	Capital Receipts to support spending plans and maximise savings in the estate and Force Risk	
	Capital Programme is insufficient to enable the investments required to meet business outcome	

When planning the audit, the following areas for consideration and limitations were agreed:

Our audit is advisory in nature and the purpose of the review is to inform the project that is scheduled to start and assist in moving the Force forward. We will specifically consider the proposed project scope for the asset management/tracking work, prioritisation and grouping. Consideration of the key processes and systems utilised to support asset management & tracking and advising regarding any benchmarking/ available best practice in this respect, together with any opportunities that may exist to better exploit existing systems within current force tech/system infrastructure.

The audit will consider the following:

- The Project Scope - we will review the project outline and provide a view as to whether the project is planned as expected;

- Purchase, delivery, receipt, recording, tagging and distribution of IT assets and specialist equipment. The focus being on identifying improvement opportunities;

- Capability of tagging the equipment issued to an individual;

- Data storage and data retention on any specialist or IT equipment;

- Collection / recovery of equipment upon an individual leaving the Force or transferring to another area/unit. Where appropriate we will consider opportunities for improvement and support (including technology opportunities);

- A record that details assets purchased/disposed/capitalised; and

- Asset checks / reconciliations / verification checks.

Given that IT has moved back in house we will understand the roles and responsibilities and will review the legacy arrangements in terms of IT/Specialist equipment and the information transferred from Boeing to identify if there are any gaps or exceptions (in relation to the scope of the audit). The focus of the audit will focus on the looking forward arrangements.

Limitations to the scope of the audit assignment:

- We will not confirm whether assets are appropriate and have been used for business purposes;

- We will not confirm the existence or location of assets, or that their valuations are correct;

- We will not perform any substantive testing, and our audit work will be based upon discussions with key members of staff and the review of policy and procedures in place.

- The results of our work are reliant on the quality and completeness of the information provided to us; and

- Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

APPENDIX B: FURTHER INFORMATION

Persons interviewed during the audit:

- Paul Ross, Head of Corporate Planning and Business Change;

- Donna Harvey, Project Support;

- Patricia Knight, Chief Information Officer;

- John Bloomer, Chief Finance Officer;

- Jasraj Purewal, Chief Accountant;

- Jonathan Gritton, Response Inspector;

- Richard Battams, Senior Project Manager;

- Andrew Chapman, Tactical Planning Unit Inspector;

- Wayne Elden, Tactical Planning Unit Officer;

- David Kelsall, Reactive Operations Inspector and Taser Lead;

- Mark Lowe, Force Armourer;

- Clare Caddick, Justice Services Chief Inspector;

- Tracey Tyler, HR System Development Manager;

- Sue Foster, HR Support Team Leader;

- David Henshall, Working at Heights and Protest Removal Lead;

- John Rainsbury, Working at Heights and Protest Removal Officer;

- Robert Neeson, Force Incident Manager and Body-Worn Camera Lead;

- Alexander Finlayson, Supplies Manager;

- Paul Prenter, NICHE Lead; and

- Steven Marsh, Chief Technology Officer.

Debrief held   14 October 2020
Draft report issued   14 October 2020
Responses received   4 December 2020

Final report issued   4 December 2020

Internal audit Contacts   Daniel Harris, Head of Internal Audit
Daniel.Harris@rsmuk.com / 07792 948767

Angela Ward, Senior Manager
Angela.Ward@rsmuk.com / 07966 091471

Client sponsor   Paul Ross, Head of Corporate Planning and Business Change

Distribution   Paul Ross, Head of Corporate Planning and Business Change
Donna Harvey, Project Support
John Bloomer, Chief Finance Officer
Patricia Knight, Chief Information Officer

rsmuk.com

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of the Police, Fire and Crime Commissioner of Staffordshire and the Chief Constable of Staffordshire, and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.