THE CHIEF CONSTABLE OF NORTH YORKSHIRE

IT Asset Lifecycle Management

Internal audit report 6.23/24

FINAL

19 March 2024

1. EXECUTIVE SUMMARY

Why we completed this audit.

The IT environment for North Yorkshire Police (NYP) is primarily on-premise, with some presence in the cloud with Microsoft 365 and Software as a Service (SaaS) providers. This results in NYP managing and maintaining a significant amount of network infrastructure. NYP is also undertaking a network infrastructure refresh to update the aging server estate. In response to the risks identified by NYP and as part of the Internal Audit Plan for 2023/24, internal audit have been commissioned to carry out this review with the object of assessing how the Force ensures that hardware and software assets are procured, monitored, maintained, and disposed of appropriately.

We planned and performed our audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions. We used a risk-based approach to select the areas of focus and the sample of items to test.

Conclusion

As a result of our review, we have identified some significant issues require management attention and noted some positive practices. NYP have a robust Digital Policing Strategy and a well-defined ICT Strategy, and both have clear aims and objectives. Additionally, the maturity of the change management approach and the capability to identify asset locations via the Internet Protocol (IP) address and the Basic Input/Output System (BIOS) demonstrates some level of control over devices.

However, we noted some significant gaps that management need to address, including the substantial discrepancies identified within the Mobiles extract from the internal ICT system (mobile phone device asset register), and inconsistencies regarding the current status of certain devices. We also detected inaccuracies within the disposals register and whilst we did receive a response that stated these gaps exist due to a natural lag in the process, we have not been able to confirm this based on the evidence we received during the audit.

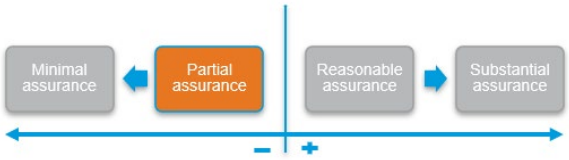
We further noted that policy documents such as the Asset and Configuration Management Policy and the Patching Policy have not been reviewed or updated since 2021. In addition, the absence of target refresh dates for devices on asset registers suggests a lack of foresight in considering the end-of-life for IT assets.

We have agreed **one high**, **five medium** and **one low** priority management actions to address the findings within this review.

Internal audit opinion:

Taking account of the issues identified, the Chief Constable of North Yorkshire can take **partial assurance** that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied or effective.

Action is needed to strengthen the control framework to manage the identified risk.



Key findings

We identified the following key findings which resulted in one high and five medium priority actions being agreed:

Asset Discovery and Logging

Our analysis found that within the Mobiles internal ICT system extract there are 255 duplicated mobile International Mobile Equipment Identity (IMEI) numbers, 1,937 duplicated SIM card numbers, and we identified 96 mobile devices noted as 'in production' with no assigned user attached. Our review further highlighted that regular reconcilliations of actual assets against registers do not occur as part of a defined schedule.

There is a risk that asset registers are not complete and accurate, which could lead to misplaced assets where devices are not properly accounted for. **(Medium)**

Asset Discovery and Logging

We inspected and conducted a comparative analysis on the disposals register and the asset register extracts from the internal ICT system and detected 37 discrepancies. For desktop PCs there are 192 disposals recorded on the disposals register and 174 marked as disposed on the internal ICT system extract. For laptop computers there are 99 disposals recorded on the disposals register, but 84 marked as disposed on the 'Computers' extract from the internal ICT system. For tablets there are 77 disposals recorded on disposals and 73 marked as disposed on the Computers internal ICT system extract.

We were advised that the differences were due to a timing difference between the asset being included on the disposals register, and subsequently removed from the internal ICT system following destruction. However, a lack of consistency and accuracy in the recording and reporting of the disposal of devices and increases the risk of mismanagement, loss, or theft of the devices. The other potential serious risk exposure is the potential for any data held within the devices that are not properly disposed of being accessed and confidential police information being obtained. **(High)**

Asset Ownership

Staff are not required to sign to accept receipt of a device. If individuals do not sign to acknowledge receipt of devices, this increases the risk that they could be misplaced or damaged, or that records do not reflect the actual owner of the asset. We further identified that there were 96 Mobile assets currently in production that did not have an owner assigned, and no individual asset owners or users had been identified on the 'Computers' internal ICT system extract.

If there is no central record of who devices are assigned to, there is a risk that they could go missing or not be returned when individuals leave the Force. **(Medium)**

Maintenance and Support

We detected inconsistencies in the status of devices on current asset registers, whereby the same devices are showing on the registers as both 'in production', 'in stock' and 'disposed'. We detected one device showing as both 'in production' and as 'disposed' on the Computers internal ICT system extract and three devices on the Mobiles extract.

The inconsistencies identified indicate a lack of reliability and integrity in the asset registers and further increases the risk of mismanagement, loss, or theft of the devices that are not properly accounted for. **(Medium)**

Asset Disposal

We reviewed the computer, mobile, network device, and server asset registers and found that no devices entered onto these asset registers have target refresh dates associated with them which could make it difficult to identify devices no longer supported by the manufacturer and therefore may be more vulnerable to cyber attacks.

The lack of planning and forecasting for replacement devices introduces the risk that they may become obsolete or inefficient over time. It also increases the risk of unexpected costs, downtime, and security breaches due to outdated or unsupported devices. **(Medium)**

Policies and Procedures

We noted that a number of key policies and procedures relating to IT asset management had not been updated for more than a year. A lack of regular reviews presents the risk that NYP may not be aware to their changing ICT landscape and may expose the organisation to the risk of outdated, inaccurate, or inconsistent policies and processes. This may affect the performance, security and reliability of IT assets and services**. (Medium)**

We identified the following controls designed and operating effectively:

The ICT Strategy sets out a clear roadmap of investment in IT assets to satisfy the needs of users and for the overarching network infrastructure required. The ICT Strategy is broken down into phases targeting continuous improvement of the ICT services and hardware provided.

The useful life of ICT equipment such as laptops, tablets and servers has been defined in policy. These have subsequently been built into the rolling programme budgeting process and ICT Strategy to allow for the timely replacement of ICT equipment that is at greater risk of going out of support and aids the maintenance of a secure technology environment.

Acceptable Use Policies for the use of the internet, email and mobile devices outlines a user's responsibilities when operating organisational ICT. This sets out ethical considerations a user must take into account and the responsibilities around maintaining the wider security control framework.

The procurement process is primarily led by the Procurement Department with input from ICT. We confirmed that NYP uses government supplier frameworks to ensure they are only purchasing equipment from reputable suppliers first cleared on frameworks such as G-Cloud. We reviewed the Core Terms defined by the Crown Commercial Service (CCS) in the purchase of Vehicle Telematics: Hardware and Software Solutions. This confirmed requirements around data protection, the vetting of staff and Security Policies in place.

We also reviewed the security assurance work that had been undertaken around the procurement of the internal ICT system, and noted the range of information requested and shared prior to engagement in the contract. Further work on the procurement process at NYP has been examined by Internal Audit in other audits and as the focus of this review was on asset management, the evidence obtained was deemed satisfactory.

2. DETAILED FINDINGS AND ACTIONS

This report has been prepared by exception Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Risk Reference: 8004			
Control	The unique identifiers for each device, such as IMEI and SIM numbers, are entered manually into the internal ICT system. Each asset is then assigned an asset tag from a pre-made roll of stickers, which is scanned. The scan automatically inputs asset details into the internal ICT system. The system allows for audits to be conducted. Scanned assets are either issued by the Service Desk or placed into storage. Quarterly visits to sites occur in order to audit devices in that location (as devices can be moved from one location to another).	**Assessment:** **Design** ✓ **Compliance** ×	
Findings / Implications	Our analysis of the mobile device asset register, which was extracted from the internal ICT asset management system, identified that there are a significant number of duplicated IMEI numbers, SIM card numbers, and 96 devices were noted as 'in production' with no assigned user attached to indicate who has received the device and is accountable for its use (see action 3). We further detected 255 incorrect entries against IMEIs and 1,937 SIM card numbers as well as duplicated asset tag numbers across the registers. These were described by management as being a result of the Lansweeper integration with the internal ICT system which has resulted in errors. Management further stated that they perform regular reconciliations of BIOSs (Basic Input/Ouput Systems); however, we were not provided with evidence of this. Our review further highlighted that regular reconcilliations of actual assets against registers do not occur as part of a defined schedule. These factors indicate a lack of accuracy, completeness, oversight, and validity in the asset registers. It also increases the risk of fraud, misuse, or theft of devices that are not properly accounted for. The Head of IT has since confirmed that the team has reviewed the asset register and identified that the duplicated instances were a result of one technician cloning entries in the database and failing to subsequently update the IMEI number for this record. The cloning process has now been updated so that it no longer copies the IMEI number, and a number would be required to be added manually instead, meaning IMEI numbers are not automatically duplicated. We have received evidence to confirm this has been amended in the system, and whilst the Head of IT recognised there is some work left to do to complete the action, the risk of duplication has been largely mitigated.		
Management Action 1	Management will perform a physical verification of all issued mobile phone devices and reconcile them with the inventory records. Management will also identify the root causes and resolve the issues relating to the duplicated IMEI and SIM card numbers.	**Responsible Owner:** Head of IT	**Date:** 31 January 2024 **Priority:** **Medium**

Risk Reference: 8004				
Control	Asset registers contain a datafield for the refresh date of ICT devices; however, these datafields have not been completed.		**Assessment:**	
			Design	×
			Compliance	N/A
Findings / Implications	We reviewed the computers, mobiles, network devices and server asset registers. The registers can capture relevant and identifiable information about devices including asset tags, manufacturer and model numbers, unique identifiers, the device status, and device type. However, we found that no devices entered onto these asset registers have target refresh dates associated with them. The lack of planning and forecasting for replacement devices introduces the risk that they may become obsolete or inefficient over time. It also increases the risk of unexpected costs, downtime, and security breaches due to outdated or unsupported devices.			
Management Action 2	Management will update the asset registers with the target refresh dates for each device and ensure they are accurate and consistent, and compare them with their target refresh dates to determine when they need to be replaced or upgraded.	**Responsible Owner:** Head of IT	**Date:** 22 December 2023	**Priority:** Medium

Risk Reference: 8004				
Control	An internal ICT system is used to record the individual to whom each device has been issued. An Internet and Email procedure statement governs the acceptable use of internet and email, and a Mobile Phones Statement covers the use of mobile telephones. However, staff are not required to sign to acknowledge receipt of a device.		**Assessment:** **Design** **Compliance**	 × N/A
Findings / Implications	The organisation does not require staff and officers to sign when taking ownership of a device, although the Head of IT explained that officers and staff are to abide by other policing policies and procedures which would cover acceptable use and information security. If individuals do not sign to acknowledge receipt of devices, this increases the risk that they could be misplaced or damaged, or that records do not reflect the actual owner of the asset. We reviewed the 'Mobiles' extract from the Internal ICT system and identified that there were 96 assets currently in production that did not have an individual user/owner assigned, and no individual asset owners or users had been identified on the 'Computers' internal ICT system extract. If there is no central record of who devices are assigned to, there is a risk that they could go missing or not be returned when individuals leave the Force.			
Management Action 3	When new devices are issued, this will be recorded accurately in the internal ICT system, and the Force will consider whether staff and officers should be required to sign to accept the device. The Force should assure itself that acceptable use (e.g. accessing unauthorised websites, safe storage of assets, etc) is fully covered by Force policies / procedures. .	**Responsible Owner:** Head of IT	**Date:** 15 January 2024	**Priority:** Medium

Risk Reference: 8004				
Control	The status of each asset (e.g. in use, under maintenance etc) is recorded in the asset registers.		**Assessment:** **Design** **Compliance**	 ✓ ×
Findings / Implications	We reviewed the asset registers for computers and mobiles and detected inconsistencies in the status of devices on current asset registers. Specifically, we detected a device that is showing as both 'in production' and as 'disposed' in the Computers asset register. For mobiles, we detected three devices showing as both 'in production' and 'in stock'. The inconsistencies identified indicate a lack of reliability and integrity in the asset registers and further increases the risk of mismanagement, loss, or theft of the devices that are not properly accounted for.			
Management Action 4	Management will implement a robust process for reviewing and updating the status of issued devices on a regular basis.	**Responsible Owner:** Head of IT	**Date:** 15 January 2024	**Priority:** **Medium**

Risk Reference: 8004				
Control	Once identified for disposal, assets are entered onto the Disposals Register. They are removed from the internal ICT system only once destruction has taken place. ICT assets are disposed of securely with third party Waste Management Provider. The third party brings an equipment shredder to site, and devices are shredded on site to a minimum of 5mm, following which a disposal certificate is issued.	**Assessment:** **Design** ✓ **Compliance** ×		
Findings / Implications	We inspected and conducted a comparative analysis on the disposals register and the extracts from the internal ICT system and found that there were discrepancies in the number of disposals recorded for different types of devices. Specifically, we found that: • For desktop PCs, there are 192 disposals recorded on the disposals register and 174 marked as disposed on the corresponding asset reigster. • For laptop computers, there are 99 disposals recorded on the disposals register and 84 marked as disposed on the corresponding asset reigster. • For tablets, there are 77 disposals recorded on the disposals register and 73 marked as disposed on the corresponding asset reigster. We were also not able to reconcile the three disposal certificates against the disposals register. We were advised that the differences were due to a timing difference between the asset being included on the disposals register, and subsequently removed from the internal ICT system following destruction. However, a lack of consistency and accuracy in the recording and reporting of the disposal of devices and increases the risk of mismanagement, loss, or theft of the devices. The other potential serious risk exposure is the potential for any data held within the devices that are not properly disposed of being accessed and confidential police information being obtained.			
Management Action 5	Management will investigate and reconcile the discrepancies within the disposals and asset registers. Management will further conduct regular audits and reconciliations of the disposal records to ensure the accuracy and completeness of the disposals register and asset registers.	**Responsible Owner:** Head of IT	**Date:** 2 December 2023	**Priority:** **High**

Risk Reference: 8004				
Control	A suite of policies and procedures in place to govern the IT asset lifecycle management processo: • ICT Strategy • North Yorkshire Police Digital Policing Strategy • Information Security Policy • ICT - Asset and Configuration Management Policy; • ICT – Asset and Configuration Management Process; • ICT - Asset Ordering Process Work Instruction; • ICT - Patching Policy; • ICT - Change Management Policy; • ICT - Change Management Process; and • Procurement Process.		**Assessment:** **Design** ✓ **Compliance** ×	
Findings / Implications	We reviewed the documents above and found that the following had not been reviewed and subsequently approved for over a year: • ICT - Asset and Config Management Policy; • ICT - Asset Ordering Process Work Instruction; • ICT - Patching Policy; • ICT - Change Management Policy; • ICT - Change Management Process; and • Procurement Process. The lack of regular reviews and approvals for policy and governance documentation presents the risk that NYP may not be aware to their changing ICT landscape and may expose the organisation to the risk of outdated, inaccurate, or inconsistent policies and processes. This may affect the performance, security and reliability of IT assets and services. Whilst each policy contained a version control, we were informed that updates had been made and tracked on SharePoint metadata, but this had not been reflected in the document's version control. In some instances the version control was updated to track changes made, however in others, the SharePoint metadata was relied on. This created an inconsistent view as to whether updates to policies and procedures had been formally approved increasing the risk that they do not reflect current, approved practices.			
Management Action 6	Management will re-assess and update the documents listed above, specifically: • Reflect current best practice. • Document future organisational requirements. • Obtain formal approval from the relevant stakeholders for the revised documents.	**Responsible Owner:** Head of IT	**Date:** 31 January 2024	**Priority:** **Medium**

Risk Reference: 8004				
	• Communicate the changes to the staff and ensure they are aware of their roles and responsibilities in relation to the policies and processes. • Establish a regular review cycle for the documents and monitor their compliance.			
Management Action 7	Management will review how to track the review and update cycle of policies and procedures and apply a consistent approach through a documented version control or using the metadata in SharePoint.	**Responsible Owner:** Head of IT	**Date:** 31 January 2024	**Priority:** **Low**

APPENDIX A: CATEGORISATION OF FINDINGS

Categorisation of internal audit findings	
Priority	**Definition**
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

The following table highlights the number and categories of management actions made as a result of this audit.

Risk	Control design not effective*	Non Compliance with controls*	Agreed actions		
			Low	Medium	High
Misplacement or theft of hardware assets, resulting in increased expenses associated with asset replacement.					
Unsupported and vulnerable systems, compliance issues, and decreased operational performance.	3** (12)	4** (12)	1	5	1
Resource wastage from unnecessary asset purchasing.					
Risk Reference: 8004					
Total			**1**	**5**	**1**

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.
** More than one management action raised against one control.

Debrief held	25 October 2023	**Internal audit Contacts**	Daniel Harris, Head of Internal Audit Philip Church, Associate Director Hollie Adams, Assistant Manager Wil Miligan, Manager, Technology Risk Assurance James Gair, Senior Consultant
Draft report issued	29 November 2023		
Revised Draft report issued	12 February 2024		
Responses received	19 March 2024		
Final report issued	19 March 2024	**Client sponsor**	Head of IT
		Distribution	Head of IT

We are committed to delivering an excellent client experience every time we work with you. If you have any comments or suggestions on the quality of our service and would be happy to complete a short feedback questionnaire, please contact your RSM client manager or email admin.south.rm@rsmuk.com

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 Chief Constable of North Yorkshire**, 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 UK 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 UK 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.