THE CHIEF CONSTABLE OF CLEVELAND

IT Asset Management

Internal audit report 2.21/22

FINAL

7 June 2021

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 / assignment and provide you with the assurances you require. It is these exceptional circumstances which mean that 100 per cent of our audit has been conducted remotely. Based on the information provided by you, we have been able to sample test the control framework.

Why we completed this audit

A review of IT asset management was undertaken as part of the agreed annual internal audit plan for 2020/21 in respect of the Chief Constable of Cleveland. IT asset management is the process of accounting for IT assets and optimising the value they provide to the organisation. IT assets represent a significant financial investment within the Force and include, but are not limited to, desktops, laptops, mobile devices and software.

The increasing prevalence of mobile technologies, the better use of data and analytics, and cloud-hosted applications can all help police officers to do their jobs more easily and spend less time filling in paperwork. Operationally, technology is enabling police forces to become more efficient in their day to day role of protecting the public. In addition, the public now expect to be able to engage with police forces digitally via multiple communication channels. Consequently, many police forces have continued to invest in technology to deliver efficiencies and align themselves to the public expectations of a modern police force.

However, whilst investment in technology provides an opportunity to meet new demands and redesign delivery models, it presents an equal challenge in terms of managing an increasingly diverse portfolio of IT assets. During the review we were informed that the Force is transitioning from an 'outsourced' IT asset management model and are currently establishing in-house processes, roles and responsibilities.

This audit was completed to provide assurance over the current processes and controls in place for managing IT assets and inform the new in-house IT asset management arrangements.

Conclusion

The Force is undergoing a transition of the IT asset management process, however, it currently lacks sufficient overview and control of their IT assets. Management recognise that there is an opportunity to improve the controls as part of the ongoing transition project. The most notable weakness is in the lack of any consolidated view of IT assets across the estate combined with no physical stock check performed that can verify the location, existence, and condition of IT assets. In addition, the Force would benefit from formalising roles and responsibilities and further clarifying processes for staff which relate to IT asset management.

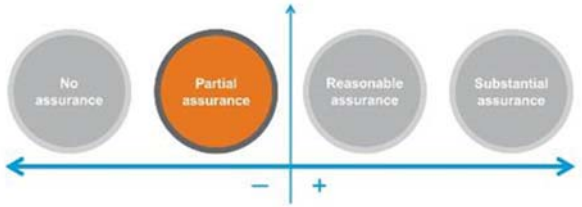
We also note that evidence we requested was not provided by management in all cases, and therefore we have agreed a finding where this is the case (e.g. leaver documentation not provided to sample test that IT assets had been recovered).

As a result of our review, we have agreed **one high** and **six medium** and one low priority actions. Details of these actions can be found in section two of this report.

Internal audit opinion:

Taking account of the issues identified, the Chief Constable of Cleveland can take **partial assurance** that the controls to manage this area are suitably designed and consistently applied.

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



Key findings

Our audit identified the following exceptions with the Force's control framework resulting in one high and six medium priority actions:

Multiple IT asset tracking sources and different teams across the Force's infrastructure, networks and desktop services are in place for managing IT assets. Information is available to show all IT assets across the estate and could be brought together if needed, but it is not routinely done and analysed. The lack of a consolidated view of IT assets across the Force's estate increases the risk that security controls are not appropriate and consistently established to manage IT assets. **(Medium)**

Work was ongoing to define the current roles and responsibilities as IT asset management is transitioned back in-house, and policies and procedures still need to be updated. This increases the risk that staff are unaware of their key duties and responsibilities, leading to asset management controls and processes not operating as intended. **(Medium)**

Regular audits/stock checks of the IT hardware assets are not completed and therefore the location and existence of assets is not fully understood and verified. This increases the risk that IT hardware assets are lost, stolen or that damage could go undetected. **(Medium)**

There are no defined processes to outline how IT asset device performance is monitored, such as those controls relating to capacity monitoring or replacement strategies to ensure that assets are not used beyond their useful economic life. This increases the risk that the Force do not detect issues with ageing IT equipment, leading to a deterioration in performance, or if assets are replaced too often wasting scarce resources. **(Medium)**

The Force use third-party waste disposal agents to securely dispose of their IT assets, however not all of the records were being signed off to confirm that checks were being made before the items were passed to the third-party disposal company. This increases the risk that the assets may still contain sensitive personal data, which may lead to a data breach, fines and reputational damage. **(High)**

The process for reporting lost or stolen devices is outlined in the Information Security Policy, however not all of the controls outlined by Management were formally documented. For example, whilst there was Lost Mobile Phone Guidance Notes there were no corresponding notes to outline the controls for laptop devices or other portable IT assets.

Further, we were not provided with the evidence we requested to validate that these controls were operating as described. This increases the risk that lost devices are not detected, reported, and the data contained within them is accessed leading to data breaches, fines and reputational damage. **(Medium)**

Leavers information was requested to pick a sample for audit testing but was not provided by Management. Consequently, we are unable to verify if this control operates effectively in practice. This increases the risk that IT assets are not recovered in a timely manner leading to unauthorised access to systems and data. **(Medium)**

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.

Area: IT asset lifecycle				
Control 1	**Missing control** The Force has an IT asset management process covering: planning, acquisition, utilisation strategy, management and disposal of IT assets.		**Assessment:** **Design** × **Compliance** -	
Findings / Implications	From discussion with the ICT Service and Operations Manager we were informed that the IT assets were historically formally managed as part of an agreement with a third party (Sopra-Steria). However, the responsibilities were in the process of being brought back in house. It was explained that there is a project (Fusion) to look at how the internal roles will be formally assigned, but this work was ongoing, and the current roles and responsibilities were not yet embedded in any job descriptions. Inspection of the asset management process confirmed 'leads' were established for the following in relation to roles and areas of responsibilities: • Laptops, desktops; • Mobile phones; and • Terminals. However, the documentation currently does not outline in any detail what the roles and responsibilities entail and what the expectations are. This increases the risk that the leads for each of these areas are unaware of their key duties and responsibilities. This could lead to these duties not being fulfilled and the asset management process not functioning as intended.			
Management Action 1	Management will ensure that the IT asset management process is updated to include as a minimum: 1. Roles and responsibilities; 2. Mechanisms for recording and tracking IT assets; 3. IT asset audits and their frequency; and 4. IT asset lifecycle process.	**Responsible Owner:** ICT Service and Operations Manager	**Date:** November 2021	**Priority:** **Medium**

Area: IT Asset inventory				
Control 2	**Missing control** The Force has an accurate consolidated view of IT assets across their IT estate.		**Assessment:** **Design** × **Compliance** -	
Findings / Implications	Inspection of the asset management process confirmed the following in relation to IT asset tracking sources: • Laptops and desktops: Microsoft System Centre Configuration Management (SCCM); • Mobile phones: spreadsheet; and • Terminals – Wyse Device Manager. We were informed that each of these device categories are managed by different teams across infrastructure, networks and desktop services. Further, there are different methods able to be used for tracking which laptop/desktop devices are in use and are connected to the network: • Cisco Prime – not yet fully implemented (70 devices only managed); and • Saracen Service Desk tool – which uses SCCM. We were informed that information to show all IT assets across the estate could be brought together if needed, but it is not routinely done (last performed April 2020). As our review was conducted remotely, due to the ongoing Covid-19 restrictions, we were unable to perform a random test to determine if the physical assets were being recorded in the register completely, accurately and timely. The lack of an accurate consolidated view of IT assets across the Force's estate increases the risk that assets are not tracked and therefore sufficient security controls are not established to manage IT assets.			
Management Action 2	Management will ensure that a consolidated IT asset inventory is maintained to include the most up to date and accurate information of staff and their equipment.	**Responsible Owner:** ICT Service and Operations Manager	**Date:** November 2021	**Priority:** **Medium**

Area: Asset audits				
Control 3	**Missing control** The Force conducts regular audits/stock checks of the IT hardware assets.		**Assessment:** **Design** × **Compliance** -	
Findings / Implications	The Force does not currently conduct regular audits/stock checks of the IT hardware assets. There is a compensating control in the form of a monthly 'computer location audit' screen, which is presented to each user at logon. The user needs to complete this to update where the asset is located. However, the lack of any physical audits means that the information provided by each user is never verified by a physical check and no active checks take place to confirm all assets are in fact logging onto the network. Furthermore, the Force does not have a process in place to track the equipment transferred between sites. There is a risk that as the Force do not conduct regular audits/stock checks of the IT hardware assets, they do not have an accurate record of hardware across the estate to apply appropriate security and asset management controls. Further, the value and cost of IT hardware could be misstated for financial reporting and insurance purposes.			
Management Action 3	Management will ensure that they conduct regular audits/stock checks of the IT hardware assets.	**Responsible Owner:** ICT Service and Operations Manager	**Date:** November 2021	**Priority:** **Medium**

Area: IT asset replacement				
Control 4	**Missing control** The Force has controls in place to monitor the performance of assets to ensure prompt action is taken to repair or replace IT assets that do not meet expectations.		**Assessment:** **Design** × **Compliance** -	
Findings / Implications	There are no defined processes to outline how device performance is monitored. In practice, issues concerning the performance of the device would be reported by an end user of the device and be logged as tickets for the helpdesk staff to progress. However, these are retrospective controls, which increases the risk that there could be disruption to services whilst the issues were resolved. No evidence was provided in relation to capacity monitoring or IT asset replacement strategies to ensure that assets are not used beyond their useful economic life. This increases the risk that the Force do not detect issues with ageing IT assets. Furthermore, the lack of any			

Area: IT asset replacement				
	agreed IT replacement strategy increases the risk that IT assets are retained for too long leading to a deterioration in performance, or assets are replaced too often wasting scarce resources. Whilst we noted that the Force has recently produced a 'Desktop Hardware Refresh Lifecycles 2020 – 2026', inspection confirmed that it failed to include the network IT assets.			
Management Action 4	Management will ensure that a formal capacity management and IT asset replacement strategy covering all IT assets is defined, approved, and implemented.	**Responsible Owner:** ICT Service and Operations Manager	**Date:** November 2021	**Priority:** **Medium**

Area: IT maintenance				
Control 5	**Missing control** The Force has no formalised maintenance plans for IT hardware, instead repairs or replacement items are purchased as necessary.		**Assessment:** **Design** × **Compliance** -	
Findings / Implications	Through discussion we were informed that the Force procures all their hardware assets from government approved procurement frameworks. The assets will typically come with a one-year manufacturer warranty, therefore any repairs within this period would be covered under warranty. The Force has explored the costs of maintenance agreements and found them to be prohibitively expensive and we were informed it was an accepted risk that devices will fail. However, we were not provided with an extract from the IT risk register or risk acceptance process (e.g. approved policy or procedure) to confirm this risk has been recorded and is approved by all relevant stakeholders. This increases the risk that management are not fully aware of the risk and are not reviewing it on a regular basis to ensure that it remains within risk tolerance levels.			
Management Action 5	Management will formally record and review the risk of not having IT maintenance plans in place to ensure that it remains within risk tolerance levels.	**Responsible Owner:** Head of IT	**Date:** November 2021	**Priority:** **Low**

Area: Secure Disposal of Assets				
Control 6	The Force has an asset management process which outlines the ICT Asset Disposal Process.		**Assessment:** **Design** ✓ **Compliance** ×	
Findings / Implications	The Asset Management Process (Section 7) outlines the approach to ICT Asset Disposal. The Force use the following waste disposal agents to securely dispose of their IT assets: • Concept Management Ltd; and • KMD Recycling Ltd. Forms are completed to seek approval for disposal, transfer assets ready for disposal and to prepare assets for disposal. A Certificate of Destruction is provided by the waste disposal agent to confirm that the asset has been destroyed securely. Examples of the equipment preparation for disposal were provided and examined. Inspection confirmed that not all of the sheets were being signed off to confirm that checks were being made before the items were passed to the third-party disposal company. This increases the risk that the assets may still contain sensitive personal data, which may lead to a data breach, fines and reputational damage.			
Management Action 6	Management must ensure that all disposal forms are signed to verify that checks have been made to make sure that appropriate preparations have been made to dispose of IT equipment.	**Responsible Owner:** ICT Service and Operations Manager	**Date:** November 2021	**Priority:** **High**

Area: Lost and stolen devices				
Control 7	The Force has outlined the approach to reporting lost or stolen devices in their Information Security Policy. The security incident response process is followed when a device is reported lost or stolen.		**Assessment:** **Design** ✓ **Compliance** ×	
Findings / Implications	Inspection of the Information Security Policy confirmed that: *'Lost computers, phones and radios are blocked by contacting the shared service centre or (out-of-hours) the control room, who will arrange for them to be blocked.'*			

Area: Lost and stolen devices				
	Management informed us that there were no recent examples we could view, but that a security incident response process would be followed for a lost device and the Information Security Team would also be notified. Management informed us that a BitLocker on laptop devices was in place to encrypt the hard drive and two factor authentication (often involving a fingerprint) is used for all other mobile devices. In addition, the Lost Mobile Phone Guidance Notes provided, explained that the device could be remotely wiped. However, not all of the controls outlined by management were formally documented, for example whilst there were Lost Mobile Phone Guidance Notes there were no corresponding notes to outline the controls for laptop devices or other portable IT assets. Furthermore, we were not provided with any evidence to validate that these controls were operating as described. This increases the risk that lost devices are not detected, reported and the data contained within them is accessed leading to data breaches, fines and reputational damage.			
Management Action 7	Management will ensure that the security controls for managing all lost or stolen devices is formally documented and evidence is retained to verify their effective operation.	**Responsible Owner:** Head of IT and Information Security Manager	**Date:** November 2021	**Priority:** Medium

Area: Asset Retrieval			
Control 8	For movers and leavers within the Force, line managers and the individuals are responsible for returning their IT assets. These processes are aligned to the HR leaver process.	**Assessment:**	
		Design	✓
		Compliance	×
Findings / Implications	Management informed us that a movers and leavers process is in place. As part of this process, users are required to return any IT assets they have received. A copy of a daily email informing system owners when staff leave (including ICT Support) was provided, which acts as the trigger to recover equipment. We requested leavers information to enable us to test the control, however this was not provided to us and therefore we were unable to verify if this control operates effectively in practice. This increases the risk that IT equipment is not recovered leading to unauthorised access to systems and data.		
Management Action 8	Management will ensure that all assets are returned when staff move or leave the Force. Regular spot checks should be performed to ensure that this happens.	**Responsible Owner:** ICT Service and Operations Manager	**Date:** November 2021	**Priority:** Medium

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.

Area	Control design not effective*		Non Compliance with controls*		Agreed management actions		
					Low	Medium	High
IT Asset Management	5	(13)	3	(13)	1	6	1
Total					**1**	**6**	**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.

APPENDIX B: SCOPE

The scope below is a copy of the original document issued.

Scope of the review

The internal audit assignment has been scoped to provide assurance on how the Chief Constable of Cleveland manages the following area.

Objective of the review
To provide assurance over the processes and controls in place for managing IT assets across the organisation.

We shall review the design and operating effectiveness of the controls across the following sub processes of IT asset management:

- **Deploy** – maintain an up to date and accurate record of all IT assets required to deliver services and ensure alignment with configuration management and financial management.
- **Manage** – identify assets that are critical in providing service capability and take steps to maximise their reliability and availability.
- **Retire and dispose** – manage assets through to disposal to ensure that assets are utilised as effectively and efficiently as possible and are accounted for and physically protected (e.g. secure destruction and disposal).

For each sub process above, we will review the assignment of roles and responsibilities, established policies and procedures, and agree with management to test a selection of key controls in place to manage the risks associated with each sub process.

Limitations to the scope of the audit assignment:

- Specifically, we have discussed with management that software licensing, value for money, and specifically police radio assets are not in scope of the review as they are currently subject to a client internal review.
- Due to the exceptional circumstances in place as a result of the Covid-19 our audit will be carried out remotely through the use of secure portals for the transfer of information, and through electronic communication means. Our review will focus on the control that operate in the organisation during normal circumstances and will not assess the exceptional controls put in place during the pandemic.
- The results of our work on reliant on the quality and completeness of the information provided to us.
- The review will be limited to identifying the existence of controls in the areas for review and obtaining supporting documentation.

- Any testing undertaken as part of this audit will be on a sample basis over a 12-month period.
- The scope of our work will be limited only to those areas that have been examined and reported and is not to be considered as a comprehensive review of all aspects of IT asset management.
- The information provided in the final report should not be considered to detail all errors or risks that may currently or in the future exist within the IT asset management environment, and it will be necessary for management to consider the results and make their own judgement on the risks affecting the organisation and the level of specialist computer audit coverage they require in order to provide assurance that these risks are minimised.
- In addition, our work does not provide an absolute assurance that material error; loss or fraud does not exist.

Debrief held	26 May 2021
Draft report issued	28 May 2021
Responses received	7 June 2021
Final report issued	7 June 2021

Internal audit Contacts	Dan Harris, Head of Internal Audit
	Philip Church, Client Manager
	Paul O'Leary, Partner, Technology Risk Assurance
	Lillian Berthung, Manager, Technology Risk Assurance
	Darren Currell, Senior Consultant, Technology Risk Assurance
Client sponsor	Chief Superintendent
	Head of IT
Distribution	Chief Superintendent
	Head of IT

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 Cleveland**, 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.