ICT Asset Management

City of York Council

Internal Audit Report 2018/19

Business Unit: Customer and Corporate Services
Responsible Officer: Assistant Director Customer and Digital Services
Service Manager: Head of ICT
Date Issued: 08 July 2019
Status: Final
Reference: 10270/001

	P1	P2	P3
Actions	**0**	**2**	**1**
Overall Audit Opinion	Substantial Assurance		

Summary and Overall Conclusions

Introduction

Asset management is a systematic process of operating, maintaining, upgrading, and disposing of assets cost-effectively. At the time of the audit, the council had 2,141 ICT assets accessed by 7,491 users.

To achieve value for money, and full use from the hardware in use, it is important that all ICT assets are tracked and managed appropriately. It is also important to ensure all ICT assets are kept updated. This is to ensure that users are using the optimal equipment and software. It is also important to ensure that assets are secure and accounted for to prevent data breaches and financial loss for the council.

Discussions with the council's ICT management have agreed that the focus of this year's audit would be a comparative review of current practice against best practice guidance. ICT management has identified the management of portable media devices as an area of risk. Therefore, whilst the audit work undertaken considered fixed ICT assets, the primary focus was on the management of portable devices.

Consideration of the chain of responsibility for portable devices was also considered. Where ICT has issued a service area with a portable device, the responsibility for that asset is transferred to the designated custodian. ICT maintains the asset register, however the management and security of issued portable devices falls outside of their remit.

Objectives and Scope of the Audit

The purpose of this audit was to provide assurance to management that procedures and controls within the system will ensure that:

- An appropriate ICT asset policy has been defined.
- ICT assets are inventoried and designated custodians have been identified.
- Information storage media are managed, controlled, moved and disposed of in such a way that the information content is not compromised.
- Users with access to and control over ICT assets have signed off on the council's Information Systems Security & Acceptable Use Policy.
- Assets are redistributed when staff leave the organisation.

Key Findings

Overall, the management of the ICT assets using asset registers and asset management software appeared to be effective. ICT assets are managed and tracked using several controls, from procurement through to end of life. Assets are assigned to the individual requisitioning the item (generally a manager as the requisition of new assets requires a budget code to be raised) unless otherwise specified. Assets are assigned asset

numbers as part of the build process, and added to the asset register when a desktop engineer (Second Line) sends the completed inventory form to the Configuration and Asset Management Analyst. All assets are configured with asset management software and can be traced using this software.

The samples tested as part of the audit highlighted how swiftly the Configuration and Asset Management Analyst can track assets and their most recent users, a control that supplements the asset register and in many cases is more up-to-date. This is due to the fact that once assets leave ICT and are handed over to the requisitioner, ICT relies on managers to keep them informed of any changes to asset ownership. This is discussed in Finding 1.

The majority of sampled disposed assets (assets marked as disposed on the asset register) were successfully traced back to the disposals master sheet. The assets that were unable to be traced were due to insufficient information recorded on the asset register. This is discussed in Finding 2.

All of the sampled smart devices were able to be traced to AirWatch[1]. The majority of the sampled laptops were traced to Snow[2], however several assets could not be traced. This is due to the caveat that Snow cannot trace assets that are not connected to the network. However, due to assets being encrypted and all new assets being marked with SmartWater[3] the risk of data breaches are reduced. It should also be noted that most data would be stored on the CYC network which could only be accessed by dual factor authentication via Citrix. This is in itself a mitigating factor.

There are three policies that relate to the management and security of ICT assets, all of which are available to staff via the intranet or documentum. The policies are updated annually and include version control information (there is evidence for the changes made to the policies, detailing any updates). The policies detail what is expected of asset users, from physical security to access control and including a comprehensive list of user requirements.

The council requires that all users of ICT assets and infrastructure have read and acknowledged the Electronic Communications Policy (ECP). Before accessing the network, users are faced with a pre-logon notification to which they must click and agree. Whilst this approach ensures that all users have acknowledged the ECP in theory, in practice the pre-logon notification is easy to ignore and users may be clicking and agreeing to it without reading what they are agreeing to (or reading the ECP). It may be worth considering changing the wording on the acceptance button from 'OK' to 'I agree'.

[1] The AirWatch Agent provides mobility management for iOS devices deployed across an enterprise. AirWatch provides ICT with the ability to enrol devices in the enterprise environment, configure and update device settings over-the-air, enforce security policies and compliance, secure mobile access to corporate resources, and remotely lock and wipe managed devices.

[2] Snow asset management software provides insight about technology endpoints – such as desktops, servers, virtual machines, mobiles, laptops, and network switches –connected to the corporate network, the applications installed on them, how that software is consumed, by whom, and when.

[3] SmartWater is a traceable liquid and forensic asset marking system (taggant) that is applied to items of value to identify thieves and deter theft. The liquid leaves a long lasting and unique identifier (unique forensic code which is registered to the council), whose presence is invisible except under an ultraviolet black light.

Overall Conclusions

The arrangements for managing risk were good with few weaknesses identified. An effective control environment is in operation, but there is scope for further improvement in the areas identified. Our overall opinion of the controls within the system at the time of the audit was that they provided Substantial Assurance.

1 Management of ICT Assets by Service Areas

Issue/Control Weakness	Risk
ICT is not informed when ICT assets change ownership within teams.	Assets without designated custodians may lead to difficulty tracking and managing the asset once it leaves the ICT team and is handed over to service areas.

Findings

The testing highlighted that once assets are handed over to service areas, they are often moved around teams without notifying ICT. 20% of the sampled assets (laptops and mobile assets) had changed users without management notifying ICT. In one instance, the asset was not able to be verified as the individual had left the council and their manager did not know where the asset was, despite the handover of assets forming part of the HR Leavers Checklist.

The handover of assets when individuals leave the council is the responsibility of team leaders. From the testing undertaken, it appears that whilst assets are being reclaimed by service areas, this process does not include updating ICT about asset ownership.

The leavers testing highlighted that the majority of assets had changed users without management notifying ICT, with 67% of the sampled assets no longer in possession of the named individual (in this case, leaver) as per the register. In one instance, the asset was not able to be traced using Snow and there is no guarantee the asset was handed back to the council.

It is acknowledged that the ICT Asset Management team have very little control over what happens to assets once they have been handed over to users. It is the responsibility of managers and team leaders to keep their own up-to-date asset registers and notify ICT of any changes to asset ownership as assets are moved around teams.

Agreed Action 1.1

The HR leavers checklist to be updated to include acknowledgement by the ICT Configuration & Asset Management Analyst that assets have been returned and re-allocated (If possible, this could be done using a self-service form on Hornbill or an email template).	**Priority**	2
	Responsible Officer	Head of HR
	Timescale	31 October 2019

Agreed Action 1.2

Hornbilll/ email form to be developed for amendments to the asset register (leavers or movers).Team leaders and managers to be reminded of their responsibilities for ICT assets	**Priority**	2
	Responsible Officer	Head of ICT

in their custody, including maintaining team IT asset registers to track assets and notifying the ICT Service Desk when assets are reallocated within teams.	**Timescale**	31 October 2019

2 Recording Replaced Assets

Issue/Control Weakness	Risk
There is inconsistency in the information recorded on the inventory form when an asset is being replaced.	Information storage media are not managed and disposed of securely, potentially resulting in data breaches and financial and reputational risk to the council.

Findings

Overall, the disposal of assets is well managed and recorded. There was a minor issue observed as part of the audit regarding the recording of replaced assets on the Inventory Form. 15% of the sample were unable to be verified as there was insufficient information captured on the asset list, due to the Inventory Form (for the replacement asset) not holding the required amount of information. Whilst the risk of misplaced assets may have serious consequences the assets identified that could not be traced were all monitors, without the capability to hold any data.

Agreed Action 2.1

Reminder to Second Line detailing the minimum required information to be included on the Inventory Form.

Priority	3
Responsible Officer	Service Desk Manager
Timescale	Completed.

Audit Opinions and Priorities for Actions

Audit Opinions
Audit work is based on sampling transactions to test the operation of systems. It cannot guarantee the elimination of fraud or error. Our opinion is based on the risks we identify at the time of the audit. Our overall audit opinion is based on 5 grades of opinion, as set out below.

Opinion	Assessment of internal control
High Assurance	Overall, very good management of risk. An effective control environment appears to be in operation.
Substantial Assurance	Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified.
Reasonable Assurance	Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made.
Limited Assurance	Overall, poor management of risk with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation.
No Assurance	Overall, there is a fundamental failure in control and risks are not being effectively managed. A number of key areas require substantial improvement to protect the system from error and abuse.

Priorities for Actions	
Priority 1	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Priority 2	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Priority 3	The system objectives are not exposed to significant risk, but the issue merits attention by management.

Where information resulting from audit work is made public or is provided to a third party by the client or by Veritau then this must be done on the understanding that any third party will rely on the information at its own risk. Veritau will not owe a duty of care or assume any responsibility towards anyone other than the client in relation to the information supplied. Equally, no third party may assert any rights or bring any claims against Veritau in connection with the information. Where information is provided to a named third party, the third party will keep the information confidential.