ICT Asset Management

City of York Council

Internal Audit Report

Business Unit: Customer and Corporate Services Directorate,
Responsible Officer: Director of Customer & Communities
Service Manager: Head of ICT
Date Issued: 9 February 2023
Status: Final
Reference: 10270/003

	P1	P2	P3
Actions	**0**	**5**	**2**
Overall Audit Opinion	Reasonable Assurance		

Summary and Overall Conclusions

Introduction

Asset management is the systematic process of operating, maintaining, upgrading, and disposing of assets securely and cost-effectively. It is essential that all ICT assets are tracked and managed appropriately to ensure council data is protected, assets are functioning as intended and achieve value for money. This responsibility is not solely that of the ICT Department as local management have stewardship duties once management responsibility passes to them. Effective asset management controls and processes are corporate requirements which include, but is not restricted to, how the council enables and supports hybrid working.

For this audit, ICT assets are defined as fixed and portable hardware devices such as computers, laptops, mobile devices, portable media devices and any other device used for IT or data management purposes. At the time of the audit, the council had over 5,000 ICT assets, accessed by over 3,000 users.

The Coronavirus (COVID-19) pandemic led to a rapid increase in the number of council employees working from home. Consequently, the focus of the ICT Department and other services was focused on mobilising the council to work very differently, with the appropriate levels of control that could reasonably be implemented given the unprecedented pace of the change and challenge faced. With more people using council-owned devices outside of the office, ICT assets and the data stored on them are increasingly vulnerable to loss, damage, mismanagement and malicious actors capitalising on the pandemic. It is recognised that as part of coming out of that initial reactive work, all departments are having to review their approach to the new controls that are required as a result of the shift in work styles/patterns. For these reasons, this audit takes into account the impacts of the pandemic, that led to the council having to adapt and work very differently at short notice, to enable the continuation of council wide service delivery.

Objectives and Scope of the Audit

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

- An inventory of ICT assets is maintained and designated custodians are identified,
- Information storage media are managed, controlled, and moved 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 and upgraded or disposed of when they reach the end of their lifecycle.

The use of and access to printers was not considered within the audit because it was considered within the scope of the Information Governance and Security audit.

Key Findings

Overall, the management of the ICT assets within the Council was found to be largely effective. When purchased, assets are assigned to the individual requisitioning the item and unique asset numbers are allocated. Once inventory forms are completed and reviewed, devices are added to the relevant inventory, depending on the asset type[1]. Assets are then configured via the relevant asset management software by ICT, enabling them to be traced using this software[2]. The use of multiple inventories and software applications is necessitated by the diversity of asset types within the Council and the division of asset management between teams within ICT.

Audit testing found that the majority of assets sampled had a fully completed and authorised inventory form. Despite this, a small number of assets recorded a duplicate asset number or other unique identifier across inventories and applications. Other identifying information, such as designated asset owner or asset location, was also found to be missing for a small proportion of assets. Departmental information has not been updated following the March 2021 Council restructure due to the frequent changes still being made to the organisational structure and the complexity of such an update. Other service areas within the Council are also facing similar challenges and ICT are currently assessing whether departmental details are necessary records for asset identification. Together, these findings partially explain why, for a sample of assets, it was challenging to independently reconcile inventory spreadsheets[1] against the relevant software applications during the audit. In other cases, it appears one of the asset management systems, SNOW, was incorrectly configured to remove 'quarantined', inactive devices after a set time elapsed.

Some of the problems faced when completing these reconciliations were also a result of changes in asset ownership within the Council. ICT is reliant on service managers keeping them informed of changes to asset ownership and managers are reminded of this throughout the HR Leaver's Checklist and Procedure. Audit testing found a similar number of laptops and mobile devices had changed hands without ICT notification as was observed in the previous 2018-19 audit of this area. It should be noted though that the use of BitLocker, dual factor authentication for Citrix, remote device wipe facilities and the '90 day check' procedure to identify, disable and delete inactive user accounts are all mitigating factors in controlling information storage media should the device be untraceable.

The Council also has a clear, comprehensive, patch management policy applicable to all information storage media. The policy and procedure were reviewed and found to meet industry best practice. However, detailed testing of patch management was not within the scope of this audit.

The Council requires that all users of ICT assets and infrastructure have read and acknowledged the Electronic Communications Policy (ECP). Detailed sample testing of whether new starters were confirming this was not completed during the audit. Nevertheless, before accessing the network, all users are required to recognise the pre-logon notification and acknowledgement of the ECP. When users are

[1] The 'Inventory Spreadsheet' maintained by the Configuration & Asset Management Analyst records all laptops, PCs, thin clients, monitors, printers and other auxiliary ICT devices. The 'Connections' spreadsheet maintained by the Print & Mobile Team Manager records all mobile phones and tablets.

[2] Atrust Device Manager records all thin clients. Microsoft Endpoint Configuration Manager and Intune record all laptops/PCs and mobile devices, respectively. SNOW records all devices that connect with the Council's network, except for thin clients.

given responsibility for ICT assets, they are also reminded of the Council's Information System Security & Acceptable Use policy, though this reminder is not documented.

Assets at the end of their useful life are identified by ICT Engineers. Records of disposed ICT assets are maintained for laptops, PCs, thin clients and associated auxiliary devices but not for mobile devices. Where records were present, they did not always contain the level of detail expected by the Council's Financial Regulations Supplementary Guidance for Asset Disposal Procedure Rules. Reconciliations of receipts from Stone ITASD (the third-party responsible for disposal of the Council's ICT assets) against the record of disposed assets and the asset registers have not been undertaken since the start of the Covid-19 pandemic due to resourcing pressures. Despite this, during the audit a sample of disposed assets could be successfully reconciled.

The Council has a range of disparate guidance outlining how to report lost or stolen ICT assets. ICT are aware of this issue and during the audit were taking steps to work with the authors of this guidance to resolve the inconsistencies identified.

Overall Conclusions

There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited. Our overall opinion of the controls within the system at the time of the audit was that they provided Reasonable Assurance.

1 Inventorying ICT assets

Issue/Control Weakness	Risk
Assets are not always consistently recorded across the Council's asset inventories. Assets do not always have up-to-date records of ownership.	Assets are mismanaged or misappropriated, leading to possible data breaches, financial loss and regulatory noncompliance.

Findings

ICT assets are recorded across various asset registers on a range of platforms, depending on the type of asset. The quality of inventory records maintained across the Council varied depending on the platform used and the type of asset inventoried.

Mobile Telephony devices

In just over half of records sampled (11/20), the information held on Microsoft Endpoint Configuration Manager did not match the information held on the Connections spreadsheet (an inventory primarily concerned with the recharging of devices to customers) or the Hornbill system (a service desk application). Most mobile device mismatches were attributed to incorrect IMEI or connection numbers. A quarter (5/20) of recorded asset owners sampled had either left the organisation (with ICT not being made aware) or, in one case, could not confirm where the sampled asset was stored.

Laptops

Similar issues were identified with laptop records during the audit. In three quarters of records sampled (15/20), the information held on Microsoft Endpoint Configuration Manager did not match the information held on the Inventory spreadsheet and SNOW (an asset management application). Most laptop mismatches were because of incorrect or absent information recorded on the manually completed Inventory spreadsheet. Occasionally, devices were found to have been inadvertently quarantined on SNOW and settings to prevent the removal of quarantined devices had not been adjusted. A quarter (5/20) of recorded asset owners sampled had either left the organisation (again, with ICT not being made aware) or confirmed they were no longer responsible for the asset.

Other devices

Where more than one asset register was maintained, records of PCs and A-trust devices were found to align across inventory records. As most PCs and all A-Trust devices do not have registered asset owners, steps were taken to identify the assets physically. Less than half of sampled PCs and A-Trust devices (7/20) could be located within West Offices. As part of the Working as One initiative the Council is in the process of re-evaluating and re-organising its ICT estate. It should be noted that the Working as One initiative was a fast-tracked programme, undertaken during the height of the pandemic and subsequent shift to working conditions within Council offices. For these reasons, the standard approach to moving large numbers of ICT devices was not followed on this occasion, with the approach being adapted accorded to circumstances.

A reconciliation was also performed between all named asset owners within asset inventories and staff leavers recorded by HR using IDEA. This reconciliation found that 231 assets were assigned to 121 staff recorded as having left the council, equivalent to 2.5% of the total population of assets across inventories. Together, these findings reaffirm the findings of the 2018-19 audit; that once an asset is handed over to services within the Council, the asset is often moved within teams without notifying ICT. This practice is in clear opposition to the HR Leaver's Checklist and Procedure, which has been updated to remind managers of the importance of notifying ICT of changes in ownership.

Agreed Action 1.1		
ICT will work with HR to review the use of Microsoft Forms as an alternative to the existing HR Leaver's Checklist ahead of taking a proposal to GRAG.	**Priority**	2
	Responsible Officer	Head of ICT; Head of HR
	Timescale	30 June 2023

Agreed Action 1.2		
Reminders will be sent to staff outlining the process for requesting the removal or transfer of ICT devices within Council offices and notifying ICT of this request.	**Priority**	2
	Responsible Officer	Head of ICT
	Timescale	31 March 2023

2 Asset identification

Issue/Control Weakness	Risk
Assets are not always assigned unique identifiers and location or asset ownership is not always recorded. This can make it challenging to distinguish and track devices.	Assets are individually indistinguishable, leading to possible data breaches, financial loss and regulatory noncompliance.

Findings

Both ISO/IEC 27001:2017 and the Centre for Internet Security CIS Critical Security Controls state that it is essential all assets have an associated unique identifier, and either an asset owner or a location recorded. The unique identifier should be separate from the assigned asset owner because an individual may hold multiple assets or transfer devices regularly. Nevertheless, all applicable devices should still have an identified asset owner to encourage user accountability for Council assets and aid device tracing. In some cases, where a unique asset owner cannot be identified, it may be practical to use device location records, such as hardware or network address, instead. In situations where a device frequently moves location or day-to-day usage is shared across a team of staff, it is imperative that a responsible asset owner can be identified for the device.

A small number of assets with duplicate unique identifiers were discovered when reviewing the Council's asset registers using the data analytics software, IDEA. The unique identifier varied depending on the asset type, but included asset IDs and IMEIs. Asset registers maintained by officers and recorded in Excel occasionally included greater numbers of duplicates but duplicates were noted across all asset registers[3]. Similarly, a small proportion of assets across all asset registers[4] did not record a named asset owner, even though a name could be recorded, such as laptops or mobile devices. At no point was this more than 1% of total assets; nevertheless, this should be rectified to ensure all Council assets remain traceable.

The kinds of location information recorded (desk number or building, directorate, IP or MAC address) varied by asset type and register. Whether location information was recorded varied significantly across registers; 21.8% of assets listed on the 'Inventory Spreadsheet' did not include any location information, whereas on Microsoft Endpoint Configuration Manager all assets included location information. During the review, it was noted that some registers only recorded either network address or physical address and across all registers directorates and departments had not been updated following the March 2021 Council restructure. As noted in the summary and overall conclusions this may reflect the dynamic and complex nature of changes needed for the move to flexible working and with the council restructure.

[3] 0.25% of unique identifiers in Atrust Device Manager were duplicates; 2.4% of unique identifiers in Microsoft Endpoint Configuration Manager and Intune were duplicates; 0.2% of unique identifiers in SNOW were duplicates. Within the spreadsheets, the 'Inventory Spreadsheet' recorded 4.5% of devices with a duplicate unique identifier and the 'Connections' spreadsheet recorded 0.14% of devices with a duplicate ID.

[4] Inventory Spreadsheet' did not have a recorded asset owner; 0.07% of mobile devices on Intune did not have a recorded asset owner and 0.71% of mobile devices on the 'Connections' spreadsheet did not record asset owners.

Agreed Action 2.1		
ICT will work with audit and an analysis of the identified duplicates will be undertaken and potential duplicates will be investigated to identify root causes and possible solutions.	**Priority**	2
	Responsible Officer	Head of IT
	Timescale	31 March 2023

Veritau

3 Lost or stolen ICT assets

Issue/Control Weakness	Risk
There is a lack of clear and consistent guidance available to staff outlining how to report lost or stolen devices to ICT.	All devices are password protected but there remains some risk that information storage media may be accessed inappropriately, before the device is able to be wiped, resulting in data breaches and reputational risk to the Council. The Council may not be aware of financial losses.

Findings

The National Cyber Security Centre's (NCSC) guidance on home working states that organisations should make sure all staff know what to do if their work devices are lost or stolen. The NCSC also recommends this guidance should be positive and blame-free to encourage staff to report losses promptly.

The procedures for reporting lost or stolen ICT assets within the Council were reviewed during the audit. Guidance to officers is available, though it is often recorded across various, tangentially related corporate policies. The guidance itself is not always clear and does not always consistently explain what officers should do when reporting losses or thefts. When reviewed against the NCSC guidance, it was found the tone of the associated policies, procedures and forms, while appropriate for those investigating the loss, did not always meet best practice recommendations.

At the time of the audit, the service was aware of these findings and work is underway, in conjunction with Information Governance and Veritau, to redesign the reporting and monitoring of lost or stolen devices.

Agreed Action 3.1

ICT will continue to develop a Microsoft Form for reporting lost or stolen assets in conjunction with Information Governance, Veritau and the Service Desk.

Priority	3
Responsible Officer	Head of IT
Timescale	30June 2023

4 Recording asset disposals

Issue/Control Weakness	Risk
Engineers do not have to record the reason for identifying assets as beyond economic repair or seek authorisation to dispose of devices. The recording of ICT assets disposals does not comply with the Council's Financial Regulations and reconciliations are not performed. Mobile devices are not securely stored whilst awaiting disposal.	Information storage media are disposed of insecurely, resulting in data breaches and financial or reputational risk to the Council. Assets may be lost or stolen.

Findings

The procedure for identifying, recording and disposing of ICT assets was reviewed during the audit. Assets are mostly identified as being 'beyond economic repair' by Service Desk Engineers when users contact the ICT Service Desk to report a fault. An Engineer will decide, using their expertise, whether the asset can be repaired cost-effectively. The reasoning behind this is not required to be recorded and the decision does not need to be authorised. During the audit there was no indication that devices had been inappropriately recommended for disposal. However, without a second approval or record of the decision this remains a risk.

The controls and subsequent audit findings surrounding recording and disposal of outdated ICT assets varied depending on the type of asset. However, it should be noted that, regardless of asset type, the details recorded and formats used do not meet the expectations outlined in Section 14 of the Financial Regulations – Supplementary Guidance: Asset Disposal Procedure Rules. This policy is also potentially misleading regarding recycling of mobile phones (section 12), as it is intended for personal mobile phones only and not council provided phones but this is not clear in the policy.

<u>Laptops, PCs, Thin Clients and Auxiliary Devices</u>
The Council maintains a register of all laptops, PCs, thin clients and associated auxiliary devices sent to Stone ITASD for wiping and disposal. In return, Stone ITASD provides disposal certificates to the Council listing all destroyed assets. At the time of the audit, reconciliations of the register and disposal certificates were paused in response to resourcing pressures imposed by the Covid-19 pandemic. Audit testing independently confirmed all assets listed on the disposal certificates were also listed on the register. Nevertheless, when the register of destroyed assets was compared to the registers of existing assets, a small percentage of destroyed devices were recorded as still existing across registers. In some cases, these devices have been identified on the SNOW system, which picks up connections to the Council's network and does not rely on officer intervention; indicating in those cases that the destruction certificate and register are both incorrect. It should be noted here that SNOW deletions are automated and occur 3 months after the last connection therefore there is the potential for disposed of assets to appear on the SNOW system during this 3 month window.

<u>Mobile Devices</u>

A register of mobile devices sent to Stone ITASD for disposal is not maintained by the Council. Although Stone ITASD provides a disposal certificate for mobile devices, without an independent, internal record of all mobile devices sent for disposal it cannot be confirmed whether all devices have been destroyed. Mobile devices waiting for disposal have been wiped of data and had SIM cards removed but they are stored in an open box within the West Offices Print Room rather than in the secure container that is available at Hazel Court. Although access to the Print Room is restricted and the room is locked when not in use, devices should still be locked away within the room.

Agreed Action 4.1		
ICT will review the existing disposals process and storage arrangements. Where necessary, ICT will update these in line with the Council's Financial Regulations. As part of this review, a second approval procedure will be developed for devices considered beyond economic repair to document approval for disposal prior to the disposal occurring.	**Priority**	2
	Responsible Officer	Head of IT
	Timescale	31 March 2023

Agreed Action 4.2		
ICT will investigate devices identified on SNOW as remaining within the organisation, despite being listed as disposed on the disposal register to identify root cause and possible solutions.	**Priority**	2
	Responsible Officer	Head of IT
	Timescale	31 March 2023

5 Identifying assets

Issue/Control Weakness	Risk
The Council does not maintain an asset classification schedule.	ICT assets are not identified and consequently ICT asset management controls and governance arrangements are not applied to these assets, potentially leading to asset mismanagement or misappropriation.

Findings

Both ISO 27001:2013 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework recommend that assets should be classified as 'ICT assets' based on the organisation's risk appetite. In this context, risk appetite refers to the extent to which devices contain sensitive information, allow access to the network, enable critical business objectives or have significant financial value. A comprehensive list of exactly what does and does not constitute an ICT asset may be challenging to update and maintain. Consequently, it is recommended that at a minimum, the de minimis level should be set. This also ensures that inefficient over-management of low risk, low value items does not take place.

The Council does not maintain a list of what constitutes an ICT asset or the de minimis level at which ICT assets are identified and tracked. Despite this, during the audit no clearly missing ICT assets were identified when reviewing the list of ICT assets recorded across the asset registers. All common, high value and high-risk ICT asset classes were fully represented across the registers.

Agreed Action 5.1

The Council will reach out to other Council ICT services to establish how they approach setting the de minimis level for asset classifications.	**Priority** 3 **Responsible Officer** Head of ICT **Timescale** 31 March 2023

Audit Opinions and Priorities for Actions

Audit Opinions

Our work is based on using a variety of audit techniques to test the operation of systems. This may include sampling and data analysis of wider populations. It cannot guarantee the elimination of fraud or error. Our opinion relates only to the objectives set out in the audit scope and is based on risks related to those objectives that we identify at the time of the audit.

Our overall audit opinion is based on 4 grades of opinion, as set out below.

Opinion	Assessment of internal control
Substantial Assurance	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable Assurance	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited Assurance	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

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.

Veritau

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.