ICT Licence Management

City of York Council

Internal Audit Report 2020/21

Business Unit: Customer and Communities
Responsible Officer: Director of Customer and Communities
Service Manager: Head of ICT
Date Issued: 05 May 2021
Status: Final
Reference: 10250/003

	P1	P2	P3
Actions	**0**	**3**	**0**
Overall Audit Opinion	Substanital Assurance		

Summary and Overall Conclusions

Introduction

A software licence is a contract between the vendor and purchaser, establishing the purchaser's right to use and distribute the software. Software licences and application maintenance are a significant area of council spend with expenditure for 2018/19 totalling over £2 million. Ineffective licence management can result in overpayment for licences that are surplus to requirements and infringement of licence agreements could result in a fine or external audit from software vendors.

The council currently utilises the Snow Software Asset Management (SAM) system. Snow is used to store an inventory of the council's Microsoft and Adobe software. It also includes discovery tools that monitor the hardware on the council's network as well as providing a repository for disposal records. Intune is the Mobile Device Management software used on the council's mobile and tablet devices.

The council's current licencing contract with Microsoft was renewed in February 2019 for £450k per annum for 3 years. The council has used this as an opportunity to move to Microsoft 365. This will change the licencing model for the council; from being charged for the number of licences deployed across the network to the number of licenced users that are active on the Microsoft portal. Consequently, ICT will need to be made aware of all new leavers to ensure the council is not overpaying for licences purchased.

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:

- The council monitors licence utilisation and deployment.
- There is an effective subscription strategy in place.
- The council complies with Microsoft licence agreement terms and conditions.
- The council only purchases the required number of Microsoft licences

Key Findings

The council has software asset management (SAM) applications and processes in place to monitor licence utilisation and deployment. There are multiple, thorough ICT policies relating to software utilisation and deployment on desktop devices in place within the council. Testing found the council held licence agreements for the majority of applications installed on their desktop infrastructure and the council complied with the terms of the licence.

Information about the licences were often recorded in spreadsheets and emails only accessible to the roles responsible for managing that area. All purchases sampled were found to be appropriately authorised in line with the council's Financial Regulations and the majority were either raised or approved by ICT prior to purchase.

The new user-based licencing approach introduced with Microsoft 365 represents a significant change to the way the council licences one of its most utilised application packages. Microsoft 365 had not been rolled out at the time of the audit, the council maintained some additional applications to perform functions that will ultimately be available through Microsoft 365. Full rollout of M365 will also provide the council with access to more updated, secure and innovative software, potentially resulting in increased efficiency and effectiveness.

Testing found that weaknesses in the council's current leaver's process may prevent the council from re-assigning user licences in Microsoft 365. The leaver's process requires managers to notify ICT of leavers but this procedure is not consistently being followed.

Overall Conclusions

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. Our overall opinion of the controls within the system at the time of the audit was that they provided Substantial Assurance.

1 Monitoring Compliance with Licencing Terms and Conditions

Issue/Control Weakness	Risk
The council does not always consistently monitor compliance with existing licence agreements across all council-owned assets.	The council may not be compliant with licence agreements they have purchased. This could potentially lead to a financial penalty.

Findings

Failure to comply with the licence agreement of the software the council uses could result in financial penalty.

Client Devices

The council use the software auditing application 'Snow'. The application has the capability to store licence terms of conditions and alert ICT's Configuration & Asset Management Team when software licences have been exceeded. The council is in compliance with the terms and conditions of the majority of licences sampled for computer-based installations.

Mobile Devices

At the time of audit the council were actively decommissioning the Airwatch MDM and replacing it with the Intune S/W provided as part of the M365 solution. This has now been achieved and the service is operating a managed whitelisting method whereby only corporately authorised applications are available to staff through their mobile devices.

Agreed Action 1.1

Microsoft along with Adobe and other applications have switched to a subscription-based model meaning, user profiles are controlled via a portal that stores all the information on licences used by the council. Snow is no longer needed to store licence information.

Priority	2
Responsible Officer	Head of ICT Support
Timescale	Completed

2 Access to Licenced Software and Applications

Issue/Control Weakness	Risk
At the time of the audit unauthorised individuals were able to access software and applications on council owned mobile devices that are not licenced by the council. Installed applications are not compatible with the council's ICT Acceptable Use Policy.	The council may not be compliant with licence agreements they have purchased. This could potentially lead to a financial penalty.

Findings

Access controls are in place to prevent unauthorised individuals from downloading or using unlicensed software on the majority of council-owned assets. Both ISO/IEC 19770-1 2017 and CIPFA's ICT Acceptable Use Policy Guidance stress the role that maintaining strong access controls has in ensuring software licences are managed and preventing noncompliance.

At the time of audit the council maintained a blacklist of applications that cannot be installed on council-owned mobile devices and blocks websites known to contain inappropriate software downloads. However, since this audit, all devices are now on Intune and CYC has adopted a whitelist approach. If people want access to additional applications they have to fill out an online form that is it is assessed by the Security Team and Information Governance Teams. This has removed the potential risk. At the time of the audit two users out of 1,384 have been able to exploit known weaknesses to bypass controls implemented within Airwatch to install blacklisted applications. A further minority of users had also installed unlicensed or inappropriate content onto devices, according to the council's ICT Acceptable Use Policy.

Agreed Action 2.1

Retire Airwatch and implement Intune alongside a whitelisting approach to application access.	**Priority**	2
	Responsible Officer	Head of ICT Support
	Timescale	Completed

3 Leaver's Process

Issue/Control Weakness	Risk
ICT is not always notified of individuals that are no longer employed by the council or partner organisations.	The council may not comply with the terms of the licence and risks fines and reputational damage.

Findings

In order to utilise the ability to re-assign, rather than re-purchase, additional user licences for Microsoft 365, ICT need to be informed of users leaving the council or other partner organisations. The council's Leaver's procedure requires managers to notify ICT of leavers as soon as they are made aware. Testing found that managers were not always following this procedure and informing ICT of new leavers.

Testing during the audit found a small proportion of users who had left the council in the preceding year retained access to the council's Active Directory. This is because ICT had not been informed that the user was no longer employed by the council. Inactive accounts should be picked up by a regular 90-day sweep of Active Directory. Accounts identified this way are suspended which prevents further access from a security perspective however, they are not de-activated until the service confirms they are no longer required, this is to ensure that those on long term sick or maternity for example do not have their accounts deleted by ICT. There is a reminder process in place to ensure that less proactive departments do not simply leave the user account active even after someone may have left however, in some circumstances this could lead to a licence not being reassigned as quickly as if the department had been more proactive in making ICT aware.

Agreed Action 3.1

An EXTERNAL master data management system has been previously developed by Business Intelligence to combine multiple streams of personnel information from individuals. ICT and Business Intelligence are working together to investigate feasibility and implement a similar INTERNAL system, working across the council (HR/Building Access/ICT) and external partners such as CYT. Reports will be produced from the system that will flag up users who have potentially no longer require access to the network or have changed roles, these reports will be sent to both users managers to take action, and be used to close various ICT/organisation processes. Feasibility will be determined over Summer 2021.	**Priority**	2
	Responsible Officer	Head of ICT Support
	Timescale	31 December 2021

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.