WELLAND INTERNAL AUDIT CONSORTIUM
Rutland County Council

INTERNAL AUDIT REPORT

ICT Asset Management

2014-15

Issue Date:	26th May 2015	***Issued to:***	Jason Haynes	Performance and Applications Support Team Manager
Author:	Lucy Fernandez		Mark Poole	Head of IT
		Agreed draft	Debbie Mogg	Director of Resources
		Final report	Helen Briggs	Chief Executive
		Final report	Saverio Della Rocca	Assistant Director – Finance

WELLAND INTERNAL AUDIT CONSORTIUM
Rutland County Council

ICT Asset Management 2014/15

EXECUTIVE SUMMARY

1. INTERNAL AUDIT OPINION

Rutland County Council's (RCC) ICT assets are managed by the in-house IT service. Effective ICT asset management is important in enabling the IT team to exercise control over IT equipment owned by the Council. This should include complete and accurate records of hardware and software. The audit was requested by the client in order to support the review of the Council's ICT strategy and operations and the development work which is already planned to strengthen the asset management arrangements.

The ICT asset management database contains appropriate data-fields to assist IT in locating items or identifying the age or value of assets; however, Internal Audit testing identified significant gaps in record keeping, these issues have been summarised in section 2 and in the action plan of this report.

Although there is a formal process in place for Human Resources (HR) to notify the IT team of starters and leavers, it was established that the ICT asset database is not periodically reconciled to current HR or Member records to confirm that ICT asset records are correct. The absence of periodic reconciliations to HR or Member records also increases the risk of failing to identify any stock that is not returned to the Council by leavers. The 'Asset Database Procedures' document states that an annual stock take audit will take place. It was confirmed that due to staff changes this has not been completed for 2014/15.

The IT team are responsible for arranging the disposal of redundant ICT assets with the selected third party organisation. The Internal Audit review confirmed that arrangements are appropriate and a review of documentation for the two most recent destruction visits confirmed compliance with the agreed process. The procurement of assets, including software, is controlled through the Council's financial procedures which have been tested in the financial audits undertaken during 2014/15. It was also confirmed that IT access controls only enable the installation of software to be completed by members of the IT team, thereby addressing the risk of installation of unauthorised software applications.

The Council does not currently hold a software application register listing details of all applications used across the authority. A complete record of all applications should be maintained and should also include details of licenses held. Reconciliations between the number of licences held and usage should also be conducted and evidenced to provide assurance over compliance with the license terms and highlight any under or over usage. Evidence was provided of such reconciliations undertaken for Microsoft software, however, this was not available for the Council's other applications.

The IT management team are aware of the need to revise the procedures for maintaining ICT asset records and it is understood that plans are in place to address this including the potential replacement of the service desk and asset management software.

Based upon the testing completed, it is the Auditor's Opinion that the current design and operation of controls provides Limited Assurance. The audit was carried out in line with the scope set out in the approved Audit Planning Record. The Opinion is based upon testing of the design of controls to manage the two risks about which the Client sought assurance.

WELLAND INTERNAL AUDIT CONSORTIUM
Rutland County Council

Internal Audit Assurance Opinion	Direction of Travel				
Limited Assurance	N/A				
Risk	**Design**	**Comply**	**Recommendations**		
			H	**M**	**L**
Risk 1: Theft, loss and misuse of Council ICT equipment and data.	**Sufficient assurance**	**Limited assurance**	1	1	0
Risk 2: Failure to manage the software in use on ICT equipment across the Council.	**Limited assurance**	**Limited assurance**	1	0	0
Total Number of Recommendations			**2**	**1**	**0**

2. SUMMARY OF FINDINGS

Risk 1: Theft, loss and misuse of Council ICT equipment and data

The Council has appropriate directive guidance available to IT staff in order to support the effective management of assets; including the safe and secure disposal of redundant assets. The 'Asset Database Procedures' document was prepared in December 2012 and last revised in September 2013.

At present all IT officers have access to the database and are responsible for updating it at each stage of an asset's lifecycle. Assets should be physically tagged and allocated a unique number; however a review of the database confirmed that seven items on the ICT asset database did not contain details of a tag. During a review of fixed assets it was noted that the council's printers had not been tagged or recorded on the ICT Asset Database. The database contains appropriate data-fields to assist ICT in locating items or identifying the age or value of assets. Details of the assets are also entered onto the 'Land Desk' Management system which enables the IT team to locate or view details of devices connected to the RCC Corporate network. Internal Audit testing did, however, identify significant gaps in record keeping.

A review of records established that as part of a project to upgrade machines, at the time of audit, the IT team were trying to trace the location of 9 PCs and 12 laptops.

Internal Audit testing also identified inaccuracies in the asset database as follows:

- Of a sample of 30 portable devices selected, 10% could not be verified as user details had not been recorded on the asset database.
- Of the 18 responses received from portable device users, 28% did not agree to details regarding status and allocated users as recorded on the database.
- Of a sample of 40 fixed assets reviewed, 17.5% of the sample had not been recorded on the asset database (consisting of telephones and printers), a further 20% of items had been recorded on the database however an inaccurate location or status was specified (items included a PC, a storage area network device, servers and monitors). The remaining 62.5% of items reviewed were found to be accurately recorded.

The structure and content of the database was comprehensive. A review of the content, however, identified 20 duplicate tag numbers, of which 9 were assigned to multiple items and 11 were double entries.

There are 326 'deployed' assets recorded with unspecified locations (e.g. laptop user/remote user/blank cell) of which 32 did not have a specific user assigned to the asset. Of the 2880 items recorded, 2078 (91%) of the items did not contain an asset value.

There is a formal process in place for HR to notify the IT team of starters and leavers; however the ICT asset database is not periodically reconciled to current HR or Member records. The absence of periodic reconciliations

to HR or Member records increases the risk of failing to identify any stock is not returned to the Council. The 'Asset Database Procedures' document states that an annual stock take audit will take place but it was confirmed that, due to staff changes, this has not been completed for 2014/15.

The IT Support Officer interviewed during the audit was aware of the procedures to be followed for purchasing assets including software; these procedures have also been formally documented in the ICT Security Policy which all staff must review as part of their induction to the Council. The procurement of assets, including software, is controlled through the Council's financial procedures which have been tested in the financial audits undertaken during 2014/15.

Risk 2: Failure to manage the software in use on ICT equipment across the Council

The Council's arrangements to effectively manage software usage are currently limited. IT management are aware of this and are intending to review the process as part of the IT service and strategy review.

It was asserted that an annual Microsoft reconciliation takes place in order to confirm that the number of users complies with the terms of the software licence. A review of documentation confirmed that this is currently taking place for 2014/15, with a completion date of May 2015. The Council does not currently maintain a software applications register which contains details of the application and its corresponding licence details (e.g. expiry dates, usage restrictions). It was therefore not known at the time of audit, without viewing actual licence documentation, whether any of the Council's other software applications have usage restrictions.

It was also confirmed that with the exception of Microsoft, use of software applications is not periodically checked by IT and reconciled to the license terms in order to monitor over or under-usage.

ACTION PLAN

Risk 1: Theft, loss and misuse of Council ICT equipment and data							
Rec No.	ISSUE	RECOMMENDATION	Management Comments	Category	Officer Responsible	Due date	WP Ref
1	Internal Audit testing identified inaccuracies in the asset database, as follows: • Of a sample of 30 portable devices selected, the details and location of10% could not be verified as user details had not been recorded on the asset database. • Of18 responses received from portable device users, the status, location or user details for 28% did not agree to details recorded on the database. • Of a sample of 40 fixed assets reviewed, 18% had not been recorded on the asset database (consisting of telephones and printers), a further 20% of items had been recorded on the database however an inaccurate location or status was specified (items included a PC, a SAN, servers and monitors). • During a review of fixed assets it was noted that the council's printers had not been tagged or recorded on the ICT Asset Within the asset database, 20 duplicate tags were identified, 9 of which had been assigned to multiple items and the remaining 11 appeared to be double entries. There are 326 'deployed' assets recorded with unspecific locations (e.g. laptop user/remote user/blank cell) of which 32 did not have a specific user assigned to the asset. Of the 2,880 items recorded, 2,078 (91%) of the items did not contain an asset value.	IT staff should be reminded of the importance of updating the database correctly as and when there are changes made. IT Management should review the database to confirm whether this is being fully completed. The errors and missing details highlighted during the testing should be investigated and resolved. In future, the value of any assets acquired should also be recorded.	Database will be reviewed in the near future with the team to highlight where this is being kept up to date and the implications of this. The intention is then for a full site audit to be conducted to ensure this is up to date before a new process is put in place so it will be kept up to date.	H	Interim Head of ICT and Performance & Applications Support Team Manager	30 Sept 2015	01.01.02 & 01.01.03

Risk 1: Theft, loss and misuse of Council ICT equipment and data							
Rec No.	ISSUE	RECOMMENDATION	Management Comments	Category	Officer Responsible	Due date	WP Ref
2	The ICT Asset database is not periodically reconciled to current HR or Member records. The 'Asset Database Procedures' document states that an annual stock take audit will take place. It was confirmed that, due to staff changes, this has not been completed for 2014/15.	IT to ensure that annual stock-checks and reconciliations to current staff and member records are undertaken.	Full audit of assets will be completed during Q2.	M	Interim Head of ICT and Performance & Applications Support Team Manager	30 Sept 2015	01.01.01

Risk 2: Failure to manage the software in use on ICT equipment across the Council.							
Rec No.	ISSUE	RECOMMENDATION	Management Comments	Category	Officer Responsible	Due date	WP Ref
3	The Council does not currently maintain a software applications register which contains details of all software applications and their corresponding licence details (e.g. expiry dates, usage restrictions). It was therefore not known at the time of audit, without viewing actual licence documentation, whether any of the Council's software applications, other than Microsoft, have usage restrictions. With the exception of Microsoft, usage of software applications and licence details is not periodically reconciled to licence information in order to monitor over or under-usage.	A software applications register should be established and maintained which clearly details software installed and corresponding licensing details and restrictions. Checks should also be conducted at the appropriate frequency to monitor over and under-usage, and to mitigate the risk that software terms and conditions are breached. Evidence of such reconciliations must be retained on file.	Agreed, currently software management system is being reviewed as part of ongoing IT review.	H	Interim Head of ICT and Performance & Applications Support Team Manager	30 Sept 2015	02.04.06 &02.04.07

GLOSSARY

The Auditor's Opinion

The Auditor's Opinion for the assignment is based on the fieldwork carried out to evaluate the design of the controls upon which management relay and to establish the extent to which controls are being complied with. The table below explains what the opinions mean.

Level	Design of Control Framework	Compliance with Controls
SUBSTANTIAL	There is a robust framework of controls making it likely that service objectives will be delivered.	Controls are applied continuously and consistently with only infrequent minor lapses.
SUFFICIENT	The control framework includes key controls that promote the delivery of service objectives.	Controls are applied but there are lapses and/or inconsistencies.
LIMITED	There is a risk that objectives will not be achieved due to the absence of key internal controls.	There have been significant and extensive breakdowns in the application of key controls.
NO	There is an absence of basic controls which results in inability to deliver service objectives.	The fundamental controls are not being operated or complied with.

Category of Recommendation

The Auditor categorises recommendations to give management an indication of their importance and how urgent it is that they be implemented. By implementing recommendations made managers can mitigate risks to the achievement of service objectives for the area(s) covered by the assignment.

Category	Impact & Timescale
HIGH	Management action is imperative to ensure that the objectives for the area under review are met.
MEDIUM	Management action is required to avoid significant risks to the achievement of objectives.
LOW	Management action will enhance controls or improve operational efficiency.

Limitations to the scope of the audit

The Auditor's work does not provide any guarantee against material errors, loss or fraud. It does not provide absolute assurance that material error; loss or fraud does not exist.

AUDIT PLANNING RECORD

Client	Debbie Mogg - Director of Resources
Assignment	ICT Asset Management

OBJECTIVES, BACKGROUND, RISKS AND CONTROLS

Critical Objectives for the area under review	An accurate and complete ICT Asset Register allows the ICT Team to exercise effective control over ICT equipment owned by the Council. This should include complete and accurate records of ICT equipment and software applications.
Background Information	The IT Audit Plan for 2014/15 has been developed to support the review of the Council's IT service and the development of an IT strategy. Responsibility for maintaining the Council's ICT assets lies with the in-house ICT team.

RISK 1	Theft, loss and misuse of Council ICT equipment and data.
Risk Description	The Council does not maintain an up to date record of ICT equipment so it is not known what ICT equipment is owned and its location. The Council is unaware of loss or theft of ICT equipment. ICT equipment is not suitably maintained. There is no procedure for procurement, disposal and disabling of ICT equipment. The Council is not able to respond to FOI requests about the Council's ICT assets.
Risk Source	Internal Audit
Sources of Assurance	Central record of each piece of ICT equipment held which includes all purchases and disposals, policy on central purchasing, financial controls to promote central spending of ICT budgets, periodic reconciliation of central record with actual equipment, controls to identify assets in need of updating/replacing.
	Preventive and Detective controls

RISK 2	Failure to manage the software in use on ICT equipment across the Council.
Risk Description	There are no procedures for procuring and installing software on the Councils network. The Council does not maintain records of software installed or details of software licences purchased. Terms and conditions of software licences are breached because an annual software to software licence reconciliation exercise is not undertaken to check under/over usage. The Council is unable to respond to FOI requests about the Council's software arrangements.
Risk Source	Internal Audit
Sources of Assurance	Software applications register and licensing information, annual reconciliation of licenses to number of users, Council procedures for procuring and installing software applications, controls to prevent unauthorised software installations on Council equipment.
	Preventive and Detective controls
Risk Source	Internal Audit

SCOPE OF ASSIGNMENT

Areas to be covered	The assignment will cover the completeness and accuracy of records relating to hardware; software; and data storage media.
Audit objective	To provide assurance that the ICT asset management arrangements are fit for purpose and registers are complete and accurate.
Audit approach	The Auditor will identify the controls in place to ensure that the Asset Register is maintained as an accurate document and carry out testing (on a sample basis where appropriate) sufficient to confirm the effectiveness of those controls. Accuracy and completeness of the controls for the management of software licenses will also be reviewed.
Benchmarking	N/A
Joint Reviews	N/A
Limitations to the scope	The Consortium's work does not provide absolute assurance that material error; loss or fraud does not exist.
Additional Client Comments	

REQUIRED DOCUMENTS & RECORDS

To enable us to commence our fieldwork we will require has access to the following information or records.
Access to or a copy of the asset register and software applications register.

MANAGING THE ASSIGNMENT

Client Sponsor	Debbie Mogg – Director of Resources
Distribution of ToR	Debbie Mogg – Director of Resources Mark Poole – Head of IT Jason Haynes – Performance and Application Support Team Manager Sav Della Rocca – Assistant Director of Finance and s151 Officer
Auditors	Lucy Fernandez – Internal Auditor
Audit Start Date	March 2015
Fieldwork Completion Date	March 2015
Draft Report Due	March 2015
Final Report Due	March 2015
Budget	**15 days**

CLEARING THE AUDIT REPORT

Distribution of Draft Report	Mark Poole – Interim Head of IT Jason Haynes – Performance and Application Support Team Manager
Discussion Window	1 week
Issue Executive Report to Client Sponsor	Within 1 week of draft report being agreed.
Agreed Circulation of Executive Report	Debbie Mogg – Director of Resources Sav Della Rocca – Assistant Director of Finance and s151 Officer Mark Poole – Head of IT Jason Haynes – Performance and Application Support Team Manager

QUALITY ASSURANCE

Document prepared by	L. Fernandez – Internal Auditor
Date	02/03/15
Document Reviewed by	R Ashley-Caunt – Interim Head of Internal Audit
Date	02/03/15
Agreed by (Client Sponsor)	D Mogg (email)
Date	16/03/15