Rutland County Council

Appendix B

INTERNAL AUDIT REPORT

the Welland Internal Audit Consortium

IT SYSTEM ADMINISTRATION 2015/16

Issue Date:	10th December 2015	***Issued to:***	Andy Nix – Head of IT
Author:	Nicola Scott		Jason Haynes – Performance & Application Support Team Manager
			Debbie Mogg – Director for Resources
			Helen Briggs – Chief Executive
			Sav Della Rocca – Assistant Director (Finance)
			Cllr King – Portfolio Holder for Place, Finance and Resources (final report only)
			Cllr MacDuff – Chair of Audit & Risk Committee (final report only)

IT SYSTEM ADMINISTRATION 2015/16

EXECUTIVE SUMMARY

1. INTRODUCTION & OVERALL OPINION

The annual Internal Audit Plan contains a number of days to cover ICT audits and is subject to approval by the Audit & Risk Committee. Potential risk areas and areas of concern are then discussed with and agreed by the Director for Resources as scope for audits in the current audit year. IT System Administration was selected as an area for review during the 2015/16 Audit Plan as it is important that the Council has effective IT System Administration of both the network and the business critical / sensitive applications. Whilst members of the IT team act as network administrators, some system administrators are based in service areas, outside of the IT team.

As all members of the IT team act as network administrators, there is sufficient cover for service users. All administrators within the IT team have their own admin accounts and any generic passwords required to access specific systems or routers are stored securely. Adequate back up procedures were found to be in place for all servers and the Council is subject to annual Public Sector Network Code of Connection compliance reviews which include a review of the adequacy of network parameters. New network users must be authorised and sample testing confirmed that these are being set up in a timely manner and with appropriate access rights. A procedure is also in place to notify the IT team of leavers so access can be promptly revoked.

Some controls were highlighted which require improvement to ensure the effective administration of the network. In areas, the testing conducted and assurances which could be given were limited due to restrictions in the availability of key information. It was identified that there are no regular reviews conducted of network users to identify any redundant user accounts and Internal Audit could not be provided with a report of all current network user accounts at the time of testing in order to verify the validity of all network access. It should be noted that if a Council leaver was to remain as an active IT user; their network access would be restricted by not having physical access to Council buildings and equipment. Review of remote access users however, did identify three leavers which still had live access to the Council's network resulting in a risk that Council records could be reviewed and altered from remote locations.

Currently the Council also does not have an IT Change Management methodology and event logs of actions by network administrators are not available. Network performance is also not recorded, monitored or reported. Internal Audit have been assured that there are already plans to address the issues identified and an action plan has been agreed with the newly appointed Head of IT.

Testing of three Council systems determined that System Administrators were aware of their responsibilities and that they have access to assistance from the IT team when required. Processes to request new users were however in some cases informal, despite relating to systems containing some sensitive data. It was noted that System Administrators are not notified of leavers from the Council resulting in a risk that access is not revoked in a timely manner. The access rights to each system were not subject to periodic review and incidences were identified where former staff retained access rights. These have since been revoked.
These issues are addressed by the recommendations in the Action Plan of the report. The audit was carried out in accordance with the agreed Audit Planning Record (APR), which outlined the scope, terms and limitations to the audit. It is the Auditor's Opinion that the current overall design and operation of controls provides **Limited Assurance**, as summarised below:

Internal Audit Assurance Opinion	Direction of Travel				
Limited Assurance	N/A				
Risk	**Design**	**Comply**	**Recommendations**		
			H	**M**	**L**
01 - The Council does not have an effective and controlled 'system administration' of its network.	**Limited Assurance**	**Sufficient Assurance**	0	2	1
02 - The Council does not have an effective 'system administration' of its business critical / sensitive applications.	**Limited Assurance**	**Sufficient Assurance**	0	2	0
Total Number of Recommendations			**0**	**4**	**1**

2. SUMMARY OF FINDINGS

Risk 1: The Council does not have an effective and controlled 'system administration' of its network.

All officers within the Council's IT team act as network administrators. The team is structured into different officer levels that in turn provide different levels of support to network users. A team calendar is in place and officer leave is managed to ensure appropriate cover. Network administration is conducted through separate, named administrator accounts set up for each member of the IT team. Whilst the use of generic user names and passwords should be avoided wherever possible, the IT team have stated that these are required in certain incidences, such as accessing routers. In these cases, the generic passwords are being saved in a secure application to which access is only given when officers have been working with the team for a period of time and a level of experience and trust has been established.

Appropriate back up procedures for all servers were found to be in place. Backups are taken at frequent intervals to hard drive and to tape, with tapes being stored securely off site. An example of successful recovery of back up data was also provided.

The Council is subject to stringent annual Public Sector Network Code of Connection compliance reviews which include the review of some network parameters such as password length and complexity.

New network users must be authorised by a line manager and testing confirmed that the users reviewed were authorised, set up in a timely manner and with appropriate access levels. New user testing was restricted, however, to only the most recent requests from the ICT helpdesk inbox as due to system limitations it was not possible to test and verify a sample independently selected by Internal Audit. The IT team are notified of leavers by an email alert from the HR Team and a diary note is created to help ensure the access is revoked in a timely manner. If the team are notified of any user who has been missed and should no longer have access to the system, the access is revoked with immediate effect.

Areas for improvements were also identified. Currently no audit trail is available of actions taken by systems administrators to network access and settings. This would result in an inability to trace and evidence the cause of an issue in the event of error or impropriety.

The Council also has no IT Change Management methodology in place and currently required network changes are recorded as help desk calls or if deemed significant classified as a project, however there is currently no guidance or

templates to outline requirements or to provide consistency. Introduction of a methodology would allow effective recording and monitoring of required IT changes and their associated authorisation, testing and implementation. An Internal Audit recommendation was made surrounding this issue in the Service Desk & Change Management Audit Report 2014/15 and discussion with the newly appointed Head of IT determined that plans are in place to address this issue.

There are no periodic reviews of all network users resulting in a risk that those no longer requiring access to the network remain as active users. As no periodic review was available and a report of all current network user accounts could not be provided to Internal Audit at the time of testing it could not be independently verified that all access related to current, bona-fide employees. It should be noted however, that if a Council leaver was to remain as an active IT user; their network access would be restricted by not having physical access to Council buildings and equipment. The Head of IT has plans to introduce monthly reports of inactive users which will identify any user accounts that need to be revoked, see Action Plan below.
The list of 359 remote access users was reviewed. Whilst the majority of users were found to be legitimate staff, Member or ICT access accounts, 19 could not be easily identified and attributed to a staff or IT user and require further scrutiny by the ICT team. A further 23 were found to be leavers, although their network access had been disabled or revoked, preventing access to Council systems. Three leavers were found to be both on the remote access list and have live network access network resulting in a risk that Council records could be reviewed and altered from remote locations. One of the leavers was also found to be an active user on one of the sub systems covered in the scope of this audit review. A summary of the remote access testing has been provided to the IT team to ensure the leavers were immediately revoked and all queries are investigated.

Performance of the network is not currently monitored or reported. Such exercises would be beneficial to both create a benchmark of 'normal' performance and allow potential problems to be proactively avoided, but also allow any issues to be detected, isolated and resolved in a timely manner.

Risk 2: The Council does not have an effective 'system administration' of its business critical / sensitive applications.

The audit reviewed the system administration of the RAISE (Adult & Children Social Care) system, FLARE (licensing) system and ELREG (Elections) system. The System Administrators sit outside of the core IT team, either within the Performance, Application & Support team or in individual service areas. The System Administrators interviewed were clear on the responsibilities which were outlined in their job descriptions and could describe arrangements to cover absences.

Testing determined that named rather than generic administrator accounts are in place and that when required administrators will contact the core IT team for support, for instance in the event that an update or patch is required. System Administrators have also developed procedures to clone the access of an equivalent user when creating a new account on their system to ensure that the access level given is appropriate to the user's need.

Some areas for improvement were identified however. Whilst the core IT team are notified of all Council leavers, currently system administrators do not receive such notification and so there is no prompt to revoke the access of such users from individual systems. This could be improved by IT forwarding the notifications they receive to a defined list of System Administrators.

Some controls were also found to be weak. For one of the systems reviewed, forms had been created to record the request for a new user to the system including authorisation of the request by line management, however in the case

of the other systems, procedures were more informal and in some cases requests were made verbally with no records available of the request or associated authorisation. This authorisation should be consistently required and evidenced when providing access to a system holding sensitive data.

It was confirmed that system event logs were available for the three systems tested, however it was also confirmed that system users were not periodically reviewed. In one case a System Administrator had carried out an ad hoc review of system users, but when this system was reconciled to HR records during audit testing some Council leavers were identified as still having current accounts on the system. These were reported and have now been revoked. System Administrators would benefit from some advice in best practice in terms of network administration, see Action Plan below.

3. ACTION PLAN

The following Action Plan provides a number of recommendations to address the findings identified by the audit. If accepted and implemented, these should positively improve the control environment and aid the Council in effectively managing its risks.

4. LIMITATIONS TO THE SCOPE OF THE AUDIT

This is an assurance piece of work and an opinion is provided on the effectiveness of arrangements for managing only the risks specified in the Audit Planning Record.

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.

Rutland County Council

the Welland Internal Audit Consortium

ACTION PLAN

Rec No.	ISSUE	RECOMMENDATION	Management Comments	Priority	Officer Responsible	Due date
1	There are no audit reports or event logs available of changes to network access and settings. This would result in an inability to trace and evidence the cause of an issue in the event of error or impropriety.	The Head of IT introduces a mechanism to record changes to network access and settings (such as changes to standing data/parameters) by network administrators, including the details of the action, time and date of the action and officer responsible.	A change control process will be introduced that will document significant changes to the ICT infrastructure. Automatic Audit logging will be investigated to see how this can help reduce risks of the inability to trace cause of issues.	Medium	Head of IT	End Jan 2016 End Feb 2016
2	There are no periodic reviews of all network users resulting in a risk that those no longer requiring access to the system remain as active users. Audit testing could not verify that all users were current employees as a report of all current network accounts was not available at the time of audit testing.	The Head of IT introduces monthly reports of inactive users to allow identification of any users whose access should be revoked. Any inactive users should be queried with HR and user access revoked if required. Such periodic reviews should also include the remote access list to ensure that leavers' remote access rights are also removed.	Monthly meetings have now been introduced to provide reports of inactive users on the network. These will be investigated with HR to establish if the access should be revoked.	Medium	Head of IT	Complete
3	Performance of the network is not currently monitored or reported.	The Head of IT should introduce a means to record, monitor and report network performance.	Where possible the performance of the network will be monitored – however this is likely to be in specific areas of concern and therefore reactive in nature	Low	Head of IT	Ongoing
4	Whilst the core IT team are notified of all Council leavers, currently system	The Head of IT introduces a system to ensure that leaver notifications are	The process for leavers will be reviewed to ensure that system	Med	Head of IT	End Jan 2016

Rec No.	ISSUE	RECOMMENDATION	Management Comments	Priority	Officer Responsible	Due date
	administrators do not receive such notification and as such there is no prompt to revoke the access of such users.	forwarded to a defined list of System Administrators.	administrators are aware of leavers.			
5	Some system administration controls, particularly in relation to system access, were found to be weak in systems that sat outside of the remit of the core IT team.	Head of IT develops and distributes best practice guidance to all System Administrators outside of the core IT team. Such guidance should include, but may not be limited to; • Authorisation and recording of user access requests and set up, especially in regards to systems containing sensitive data; • Periodic user access reviews; • Ensuring audit log functionalities are activated on all systems.	A best practice guide will be produced and system administrators asked to complete a questionnaire regarding system administration.	Med	Head of IT	End Feb 2016

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 Recommendations

The Auditor prioritises 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.

Priority	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.