Report to:	**Audit, Best Value and Community Services Scrutiny Committee**
Date of meeting:	**17 March 2015**
By:	**Assistant Director - ICT**
Title:	**Network Leavers & Transfers Audit 2014/15: Progress Report**
Purpose:	**An update on work being carried out to reduce the current partial assurance position of the Leavers & Transfers audit review**

RECOMMENDATIONS

1) To note that the outstanding recommendations 1, 3 and 4 have been addressed and the associated risks removed.

2) To note that mitigating actions have been taken to minimise the risk exposure relating to recommendation 2 concerning the personnel management of third parties.

---

1 Background

1.1 The review audit into staff transfers and leavers, although improved, again returned an audit opinion of partial assurance. This report explains the work underway to address that position and remove / mitigate identified risks.

2 Supporting information

The current position of the four outstanding recommendations resulting in the opinion of partial assurance is described below. Recommendations 1, 3 & 4 are resolved; recommendation 2 has been addressed through a set of mitigating actions and will continue to be addressed:

Recommendation 1

2.1 *"The process for managing staff transfers still requires completion of two separate forms and the intranet guidance on staff transfers does not make this clear. The need to complete two forms for the same process is considered to be confusing and inefficient and could lead to delays in setting employees up in their new roles."*

Update: Presently there remains a need for two forms to cater for individuals that may have more than one job within the County Council to handle the subtle differences of a discreet personnel contract ending and another commencing alongside a continued network presence, albeit with different access rights. However, the audit requirement has been addressed; the intranet guidance surrounding this process has been changed to make this necessity clear and both personnel and ICT forms have been simplified. The Personnel Intranet page has also been amended to include the following text to assist with sign-posting managers:

"When an employee already has access to IT systems and transfers to a new role with the County Council, their line manager needs to complete a Change / Transfer Network Account form available on the ICT Portal."

Recommendation 2

2.2 *"Since the previous audit review, a control has been introduced to review SAP leaver records for ESCC employees retrospectively and to disable any network accounts that have not been processed correctly. However, at the date of this review, we found that there is no control in place to perform a similar review for contractors, agency staff and other third party staff such as Amey, May Gurney and Public Health employees. As a result, there is still a risk of individuals leaving but continuing to be able to access their network account."*

Update: The existing SAP based controls can only be applied if an individual is contracted to work for ESCC; in this instance, there will be a personnel record in the HR part of SAP and this will be picked up by the leavers disabling procedure. Contractors working for ESCC do not appear in the HR part of SAP but will be paid through the Finance part of SAP. However, if an individual is neither employed directly by ESCC in SAP nor paid via SAP, there is no overall personnel control to manage the starter / leaver process. Amey, May Gurney, Public Health and increasingly partners, such as Surrey, fall into this category.

ICT manages network rights via a directory system (Active Directory); its purpose is technical control, not a personnel management system. Once such third party accounts are set up in the directory, they are indistinguishable from other ESCC users.

ICT has put in place a number of controls in order to mitigate the risk of unauthorised access to sensitive and confidential information in relation to agency staff and partner system access beyond the period of their contracted period, as follows:

- The network accounts of these leavers are controlled by setting them to expire at contract end. If a contract is extended, the associated network account can only be extended by the employing line manager and then again, only to a specified end date.
- All Active Directory accounts are automatically disabled after 30 days of inactivity.
- The leavers' protocol for physical access to Council buildings is a physical control that should prevent unauthorised personnel from logging onto a computer on the Council network during the 0-29 day period of inactivity.
- Remote access to the Council's network, using the portal or Virtual Private Network client software, requires the use of a two-factor authentication token. The leavers process places a requirement on the contracting manager to retrieve the token on the last day of the contract and return it to ICT services. This is specifically mentioned on both the PAT Leavers Checklist and Agency/Contractors Leavers Checklist.
- ICT has established a register of third parties and has instigated dialogue with representatives and contract managers of these partners. There is further work to be done to verify current staff and instil ownership of the process with this officer group.

ICT and PAT will also initiate an awareness raising campaign directed at managers that appoint contract and other interim professional services. The campaign will use the intranet and social media and will highlight the responsibilities of managers in the starters, transfers and leavers process. This will draw specific attention to the responsibility of managers to notify ICT of any departures or transfers which would necessitate changes to system access.

It is the view of the ICT Service that the above controls are proportionate and provide sufficient treatment of the identified risk. It should be noted that the Council's approach to ICT security was tested in January 2015 during the recent PSN (Public Service Network) Code of Connection application. The Cabinet Office confirmed that the application was successful and that the Council meets the requirements of connecting to the PSN.

Recommendation 3

2.3 *"When staff transfer into a new position, access rights to the former team network folders should be removed, however, we found examples where staff had transferred into new positions but could still access their former teams network folders. We recommended that ICT should investigate options available for line managers to monitor and control who has access to their team's network folders. However, this recommendation has not been progressed and line managers are only able to view the groups that have access to folders rather than individual users. Until line managers can monitor and manage who has access to their network folders, there is a risk of sensitive or confidential information being compromised."*

Update: The new ICT Service Management tool now controls this risk. Any request for a Change in a Network Account now revokes all previous access and amends the new access to that specified by requesting line manager. This includes revoking access to previous team mailboxes and data. If any access is still required to these items, a separate New Request, is required from the person with ownership.

Recommendation 4

2.4 *"We found that it was possible to amend the ICT change request form (Network Account Form) and make it appear that the request had come from the employee's line manager. Whilst change request forms are reviewed and approved by ICT Business Solutions, the review process would not identify forms that had been deliberately amended to conceal the name of the person making the request. As a result, there is a risk of unauthorised additions and changes to permissions being made leading to an individual having inappropriate access to sensitive information and potentially gaining inappropriate access to other systems. However, we understand that the replacement for the Remedy System, which is due to be implemented in October 2014, will address this problem by preventing someone from changing the request to make it appear to have come from someone else."*

Update: This recommendation was about ensuring that requested changes have been properly authorised by those that own the information. The implementation of *My ICT,* the new self-service ICT portal has resolved this issue completely.

3. Conclusion and reasons for recommendations

3.1 This report explains how outstanding audit recommendations 1, 3 and 4 have now been addressed.

3.2 In the case of recommendation 2, the report sets out a set of mitigating controls that have been put in place to manage the risk and negates the need to interconnect the Active Directory system with SAP and third party databases holding contractor and agency details.

Matt Scott
Assistant Director ICT

Contact Officer: Nicky Wilkins
Tel. No. 01273 337332
Email: nicky.wilkins@eastsussex.gov.uk