Follow Up of the Audit of Access to Key IT Systems Memorandum Report City of York Council

For: Assistant Director Customer Services and Digital, ICT Infrastructure Manager and ICT System Support Team Leader
Status: Final
Date Issued: *16 March 2018*

1 INTRODUCTION AND SCOPE

1.1 ICT plays a key role in the efficient delivery of services to the public, and is also vital to the effective internal operation of the Council. New technologies bring clear benefits, but also bring with them new obligations and areas of risk exposure.

1.2 Organisations must ensure that electronic information is held securely to prevent disruption to services, and personal data fall additionally within the scope of the Data Protection Act 1998. Compliance with the principles in the Act is monitored by the Information Commissioner's Office (ICO), which since 2010 has regularly imposed fines on organisations for failure to comply. The ICO has the power to levy fines of up to £500,000.

1.3 Ensuring that access to data is restricted to authorised persons is therefore of vital importance to organisations. In the event of an information security breach, they must be able to demonstrate that as far as possible they had put in place appropriate procedural and technological security measures to manage risks.

1.4 The original audit was finalised on 18.04.17, giving an overall opinion of Reasonable Assurance.

Objectives

1.4 The objective of this follow up audit was to provide assurance to management that procedures and controls over key council systems will ensure that access to data is restricted to authorised users. The following systems were covered by this audit:

- iWorld - Revenues and Benefits, Housing Rents;
- FMS - Civica Financials;
- Servitor - housing repairs management; and
- Frameworki - Adult Social Care.

This included a review of procedures for creating and removing user accounts, settings for passwords and other access control features. As the Mosaic system was newly implemented after the original audit testing, arrangements for authorising remote access by third parties were also reviewed in this case.

Key findings

1.5 Testing demonstrated that the vast majority of agreed actions have been implemented, though there have been some issues implementing the actions for Servitor, due to the limitations of the system.

2 FINDINGS

Shared and non-human user accounts

2.1 Mosaic

The previous audit found that there were some non-human user accounts on Frameworki, (the antecedent social care system) which appeared never to have logged onto the system. These were investigated during the course of the audit to determine whether they were necessary and whether they had any inappropriate permissions. It was agreed that the same authorisation process for non-human accounts would be implemented as for human users.

2.2 Non-human accounts must now be authorised via the self-service portal, in the same fashion as human users.

2.3 There is a corporate approach to the authorisation of supplier accounts and this is applicable to Mosaic. Suppliers are given access via Entrust. Their accounts are disabled after use and are enabled when access is required. CYC issue them with a PIN which they are required to enter as part of the authentication process.

2.4 iWorld

The original audit found that there were several non-human accounts with considerable rights. These were removed during the course of the audit. In addition, it was agreed that the same authorisation process for non-human accounts would be implemented as for human users.

2.5 A reduced number of non-human accounts are now in operation with defined purposes. Non-human accounts must now be authorised via the self-service portal, in the same fashion as human users.

2.6 Servitor

The original audit found that the system administrator account 'HOUADMIN' was shared by around ten IT administrators. It was agreed that the possibility would be investigated of assigning administrators individual accounts. In addition, it was agreed that the same authorisation process for non-human accounts would be implemented as for human users.

2.7 Administrators now have individual accounts to ensure accountability. Non-human accounts must now be authorised via the self-service portal, in the same fashion as human users. The 'HOUADMIN' account has now been disabled and individual accounts assigned to administrators.

2.8 FMS

The original audit found that the creation of non-human user accounts was not required to be authorised. It was agreed that the same authorisation process for service accounts would be implemented as for human users.

2.9 Non-human accounts must now be authorised via the self-service portal, in the same fashion as human users.

New user requests

2.10 Mosaic
The original audit found that the request process for Frameworki was informal, with some sent via the self-service function and some to the IT helpdesk. Some specified the required user group and some did not. It was agreed that a standard new user/amend user form would be adopted for Mosaic.

2.11 It was found that all requests for new users and amendments to Mosaic user accounts are now submitted on a standard form via the self service function. The form mandates specification of a user group and must be approved by a relevant manager. This ensures consistency of group access levels and of the authorisation process.

2.12 iWorld
The original audit found that the request process for iWorld was informal, with some sent via the self-service function and some to the IT helpdesk. Some specified the required user group and some did not. It was agreed that a standard new user/amend user form would be adopted for iWorld.

2.13 It was found that all requests for new users and amendments to user accounts are now submitted on a standard form via the self service function. The form mandates specification of a user group and must be approved by a relevant manager. This ensures consistency of group access levels and of the authorisation process.

2.14 Servitor
The original audit found that the request process for Servitor was informal, with some sent via the self-service function and some to the IT helpdesk. Some specified the required user group and some did not. It was agreed that a standard new user/amend user form would be adopted for Servitor.

2.15 The ICT service are in the process of designing a new user form for Servitor. In the meantime, a basic user request form has been adopted and can also be accessed via the self-service function. Appropriate authorisation must still be obtained for new users or amendments to user accounts.

2.16 FMS
The original audit found no issues in this area in relation to FMS. Requests for new users continue to be submitted on standard forms via the self service function. The form mandates specification of a user group and must be approved by a relevant manager.

Account security settings

2.17 Mosaic
Mosaic uses Active Directory Authentication. A server running Active Directory Domain Services authenticates and authorizes all users and computers in a Windows domain type network. Applications can be integrated into this authentication protocol and users do not therefore require

separate passwords or usernames for the applications. This protocol requires passwords of sufficient length and alphanumeric complexity.

2.18 iWorld
The original audit found that password settings were weak, specifying a minimum of only five characters and failing to enforce alphanumeric complexity. It was agreed that more complex password settings would be introduced.

2.19 iWorld now requires a password of sufficient alphanumeric complexity and must contain a minimum of eight characters.

2.20 Servitor
The original audit found that system administrators were unsure of the password security settings, but did state that they didn't expire and could be text only. It was agreed that a process of implementing more complex passwords would be investigated.

2.21 Improving password complexity is not possible at this time due to software limitations. Options for software upgrade or replacement are currently being investigated.

2.22 FMS
FMS continues to use Active Directory Authentication. A server running Active Directory Domain Services authenticates and authorizes all users and computers in a Windows domain type network. Applications can be integrated into this authentication protocol and users do not therefore require separate passwords or usernames for the applications. This protocol requires passwords of sufficient length and alphanumeric complexity.

User security reviews

2.23 All four systems
It was found that whilst six monthly management reviews were undertaken to ensure that user access was still appropriate, the resulting information was not stored methodically and it was not possible to determine how the managers' responses were monitored at a detailed level. It was agreed that a standard template would be adopted to record the checks and actions carried out as result.

2.24 Six monthly management reviews continue to take place. The ICT service have chosen not to adopt a template for the recording of the resulting account amendments, as any changes to accounts are already recorded separately. However, measures have been adopted in order to ensure the consistency and efficacy of the review. In the event of non-response, accounts are now deactivated until managers confirm that the access levels of their staff are appropriate. All email correspondence is retained as evidence.

3 CONCLUSIONS

3.1 Good progress has been made since the previous audit and the majority of the agreed actions have now been implemented. Controls are in place to prevent unauthorised access to the Mosaic, iWorld and FMS systems. These controls include individual administrator accounts to ensure accountability, standardised user forms which require appropriate authorisation, password settings of sufficient length and alphanumeric complexity and regular review of the appropriateness of user access.

3.2 Individual accounts are now assigned to Servitor administrators and regular reviews are undertaken to ensure user access remains appropriate. Whilst a standard new user form is still in development, new users can only gain access to the system via a basic request form which is authorised by a relevant manager.

3.3 Due to system limitations, more complex password settings cannot be implemented on the Servitor system. Options are currently being explored for system upgrade or replacement, providing the capability for stronger account security settings.

APPENDIX 1 – ACTIONS AGREED TO ADDRESS CONTROL WEAKNESSES

Action Number	Report Reference	Issue	Risk	Agreed Action	Priority*	Responsible Officer	Timescale
1	2.15	New user forms are still in development for Servitor.	Inappropriate and / or unauthorised access to data and systems.	At the time of issuing the final report, the new user forms are now in operation on the self-service portal.	2	N/A	N/A
2	2.21	The current version of Servitor does not allow for appropriately complex password configurations. The system requires to be upgraded or replaced.	Inappropriate and / or unauthorised access to data and systems.	The upgrade of Servitor to a version which allows more granular management of passwords has been considered and senior management have decided not to do this at present. The upgrade is valued in excess of £50k and, as the system is part of a wide Housing service review and may be replaced, it has been decided not to spend this money until the outcome of this review is known. At this point, the Servitor	2	ICT Infrastructure Manager (PR) Business Engagement Manager (AC)	Sep 19

				system will be either be upgraded or replaced. In either case, password complexity will be improved.			

*The priorities for actions are:

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.