Access to key IT systems

City of York Council

Internal Audit Report 2016/17

Business Unit: Various
Responsible Officer: Various
Service Manager: Various
Date Issued: 18th April 2017
Status: Final
Reference: 10245/004

	P1	P2	P3
Actions	**0**	**11**	**4**
Overall Audit Opinion	Reasonable Assurance		

Summary and Overall Conclusions

Introduction

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.

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.

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.

Objectives and Scope of the Audit

The purpose of this 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 systems covered by this audit were:

- 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, along with remote access by third parties such as suppliers. The fieldwork was carried out during 2016.

Key Findings

The council generally has good processes in place to manage the aspects detailed above. To be able to access to the systems reviewed, a user must possess a valid domain username and complex password in line with Public Services Network requirements. Three of the four systems reviewed require them to have an additional valid username and password for the applications themselves.

These provisions offer generally good control over user access, but we found that some systems' password settings are weaker than desirable, or have not been fully investigated by the council.

Some processes for authorising and controlling several systems' user accounts have not been formalised, which generates unnecessary work for the service desk staff and could lead to confusion over access levels required.

There are also various shared accounts in use and several non-human system administrator accounts in use, which are not subject to the same authorisation process as standard user accounts, and the use of which reduces individual accountability. Some of these have already been removed.

Overall Conclusions

It was found that the arrangements for managing risk were satisfactory with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made. Our overall opinion of the controls within the system at the time of the audit was that they provided Reasonable Assurance.

1 Shared and non-human user accounts

Issue/Control Weakness	Risk
Unique accounts are not always provided for users, including administrators. The creation of non-human user accounts is not required to be authorised.	Lack of accountability for users' actions when using shared accounts. Unauthorised persons gain access to data or make changes to council systems.

Findings

We identified several Frameworki non-human users which appear never to have logged on: DASMAN, OMONITORING and CSUPPORT. The email address attached to OMONITORING relates to a user who also has an account in her own name.

From the list of iWorld users supplied, we identified twelve on the FIRST-DEFAULT profile and fifty-five on the RB-SYSADMIN profile. These are profiles with considerable rights. We queried whether all of these were necessary with administrators and were informed that many were redundant. They were removed during the course of the audit.

We identified: stodba and Ops$Walkthrough, which are Servitor non-human users and were advised that these are used by the database administration team and automated processes run using these users. Generic human users are: FRAUD1 used by the Veritau Fraud Team and HOUADMIN, which is shared by around ten IT administrators. We were informed that these are used because Servitor licences are expensive and the council operates a "one in, one out" licensing policy to stay within a restricted number of licences and avoid incurring additional costs.

Making accounts available to multiple staff makes it more difficult to establish or trace accountability. The shared use of the administrator account creates a particular risk, and if shared accounts are deemed necessary for cost reasons, the council could consider reducing this risk by providing administrators with individual accounts and creating lower risk shared accounts e.g. view only or similar.

Our sample testing of new user accounts also identified that authorisation is not required for the creation of system support admin user accounts. Examples found were “REPORT” (Servitor) and “Systems and Development, Resources” (FMS).

Agreed Action 1.1 - Frameworki

The users identified above were investigated and found the following:

The worker name ‘OMONITORING’ is a system worker used by the Intensive Support

Priority	2
Responsible Officer	ICT Systems Support Team Leader

Team within Adult Social Care. The role has never been logged into and the password has never been given out but it is an account that needs to be kept in the system. The email address allocated to the worker is not necessary but enables the ICT System Support to have a contact person for this system worker. The role enables the Intensive Support Team to have a holding account for all the outcome monitoring work and allows the service manager to allocate the client support requests to individual workers within the team.	**Timescale**	Implemented
Agreed Action 1.2 - iWorld		
All 55 users with profile RB_SYSADMIN have been either disabled or moved to the ALL_USER profile. The same authorisation process for service accounts will be implemented as for human users.	**Priority** **Responsible Officer** **Timescale**	2 ICT Systems Support Team Leader 31/05/2017
Agreed Action 1.3 - Servitor		
The possibility will be investigated of assigning administrators individual accounts. The same authorisation process for service accounts will be implemented as for human users. Licence implications and significant cost if systems support require individual named user accounts. A management decision to keep the current status has been taken.	**Priority** **Responsible Officer** **Timescale**	2 ICT Systems Support Team Leader 31/05/ 2017
Agreed Action 1.4 - FMS		
The same authorisation process for service accounts will be implemented as for human users.	**Priority** **Responsible Officer** **Timescale**	2 ICT Systems Support Team Leader / ICT Infrastructure Manager 31/05/ 2017

2 New user requests

Issue/Control Weakness	Risk
Formal user management processes were not in place for the creation of new Frameworki, iWorld or Servitor user accounts or for revisions to them. Using model users means that access level errors may be duplicated.	Inappropriate and / or unauthorised access to data and systems.

Findings

We reviewed a sample of new users for each of the systems and examined how access was requested.

The request process for Frameworki, iWorld and Servitor is informal. Specific request forms are not used and instead requests are sent as emails to the service desk or are raised using the online self-service function. One request included an "Interim Frameworki Change Request Form", which is not intended for this purpose. Some requests indicate a model user, whose access level should be copied, while others specified a role, although the correct role name was not always given in the request. Requests do not always initially come from the appropriate authorising manager, and as a result service desk staff sometimes have to enter into lengthy chains of correspondence relating to a request, before all queries have been addressed.

When permissions are modelled on those of an existing user, such as those of the officer who is being replaced or who carries out the same duties, this can duplicate existing permissions errors if the permissions/roles/access levels have never been subject to a fundamental review of their capabilities.

The introduction of system-specific user request forms and the requirement for all user requests to be authorised and then directed to the service desk could streamline the process for creating new users. If it required roles or modules to be confirmed positively rather than a model user to be nominated, this could also ensure that future records and authorisations for user accounts are centrally maintained and stored.

For the FMS system, new user requests must be submitted on a unique form. Forms were available for all users samples, except for the system admin account mentioned previously and a user whose form could not be located. All forms had been appropriately authorised with the exception of one on behalf of an external auditor.

The list of FMS new user authorisers was out of date at the start of the audit, although it was updated after this was pointed out by the auditors carrying out the Main Accounting System audit.

Agreed Action 2.1 - Frameworki		
Mosaic Adults replaced for Frameworki in November 2016. There is a new/amend user	**Priority**	2

form for Mosaic Adults. A new user form for access to Mosaic Childrens and Careworks has been created. All new users or changes to users require Service Manager approval.	**Responsible Officer**	ICT Systems Support Team Leader
	Timescale	Implemented
Agreed Action 2.2 - iWorld		
Specific user request forms for iWorld will be adopted.	**Priority**	2
	Responsible Officer	ICT Systems Support Team Leader
	Timescale	30/06/ 2017
Agreed Action 2.3 - Servitor		
Specific user request forms for Servitor will be adopted.	**Priority**	2
	Responsible Officer	ICT Systems Support Team Leader
	Timescale	31/05/2017

3 Account security settings

Issue/Control Weakness	Risk
The council has not made a risk-based decision on system password protection. Some security settings may not be strong enough for the sensitivity of the data being secured. Servitor security settings have not been explored. Some iWorld users have identical passwords.	Inappropriate and / or unauthorised access to data and systems.

Findings

It is important to note that all users are required to authenticate to the CYC network before accessing any of the systems which we reviewed. A user must therefore possess a valid domain username and complex password in line with Public Services Network requirements. Specific issues with each system's own security settings are identified below.

The Frameworki password complexity follows the settings used for SQL Server 2005. These are broadly in line with Public Services Network and/or Microsoft requirements or best practice, although "Store passwords using reversible encryption" is enabled. Microsoft specifies that this should never be enabled, unless it is required for a specific purpose. The minimum password age of 0 days is also low, but as the password history setting is high at 20, it is very unlikely that a user would reset their password 20 times in immediate succession to get back to their original password.

Notes covering the new user process are available, but this guidance did not include any instruction to force the new user to change their password when they first log on. We were informed that this was changed during the audit.

For iWorld users except the system administrator accounts, some password settings are particularly weak: minimum password length is only five characters and no alphanumeric complexity is enforced. The maximum password age is 90 days, which is relatively long, given the sensitivity of the data. It is believed that all password settings are unchanged from the defaults for the system. The system administrator accounts cannot be locked out, their passwords do not expire and have fewer characters. Again no minimum alphanumeric complexity is enforced. However there is a justifiable reluctance to change these, as this may affect automated process functionality.

We were provided with a report of all iWorld users which included passwords in encrypted form. This revealed that some clusters of users have identical passwords. We would advise that this issue is investigated further. We also found that not all passwords were encrypted; although

the guidance notes flag that encryption should be enabled. This has already been addressed for all accounts except systems accounts which may affect functionality.

For Servitor, administrators were unsure of the password configuration and could not provide screenshots, but did state that they do not expire, can be text only and users are locked out if they enter an incorrect password too many times. No other settings such as minimum length were known. Administrators have sought further details from the supplier.

We also noted that administrators keep a record of all users' passwords in a spreadsheet when they are created, and users are not prompted to change them at first log on. Thus we were able to determine for example that some passwords were only three characters long and "password" can be used as a password. This indicates that the security of password settings is weak.

The Civica FMS system does not have its own authentication process and uses Active Directory authentication, so users do not have to enter a separate password to gain access. As noted in the Frameworki findings above, these are in line with best practice apart from “Store passwords using reversible encryption” being enabled.

We would advise that password settings for these systems are reviewed, and the council makes and documents a decision on the strength of security settings, based on the level of risk which the council feels is attached to the data in each system. The council has a policy on Active Directory security settings, but does not have a similar documented approach to the security of individual applications.

Agreed Action 3.1 - Frameworki

Mosaic Adults went live on 14th November 2016 – Frameworki is now redundant. Mosaic Adults uses Active Directory authentication.	**Priority**	2
	Responsible Officer	ICT Systems Support Team Leader
	Timescale	Implemented

Agreed Action 3.2 - iWorld

Implemented more complex password on 9th May 2016 after a system update which made this possible – these must now be a minimum length of 8 characters and must include the following: • Uppercase character • Lowercase character • Number • Special Character	**Priority**	2
	Responsible Officer	ICT Systems Support Team Leader
	Timescale	Implemented

Agreed Action 3.3 - Servitor

A process of implementing more complex Oracle passwords is now possible and has been carried out.

All non-super user account passwords will be a minimum length of 8 characters and must include the following

- Uppercase
- Lowercase
- Number
- Special Character

Unable to change the main HOUADMIN password as this has operational database consequences.

Priority	2
Responsible Officer	ICT Systems Support Team Leader
Timescale	Implemented

Agreed Action 3.4 - FMS

This will continue to use Active Directory authentication.

Priority	2
Responsible Officer	ICT Systems Support Team Leader
Timescale	Implemented

4 User security reviews

Issue/Control Weakness	Risk
Ability to monitor the effectiveness of reviews is limited.	Inappropriate and / or unauthorised access to data and systems.

Findings

ICT send lists of users and their permissions to appropriate managers every six months and request that their access is confirmed as valid.

These checks are one of the key controls covering user permissions levels and were introduced by ICT to compensate for an apparent lack of accurate information on leavers and internal movers being provided to them.

We requested information on these checks and found that there was evidence of them being carried out regularly. However the information for each system was not stored methodically and it was not possible to determine how the managers' responses are monitored at a detailed level.

For example, we could not readily examine how thoroughly individual managers check that their users are valid or how many accounts were amended as a result of the checks.

Agreed Action 4.1 - Frameworki		
A standard template has been adopted to record the checks and actions carried out as result. Three reminders will be sent to managers and if a response is not received, access will be removed for any unconfirmed users.	**Priority**	3
	Responsible Officer	ICT Systems Support Team Leader
	Timescale	Implemented

Agreed Action 4.2 - iWorld		
A standard template has been adopted to record the checks and actions carried out as result. Three reminders will be sent to managers and if a response is not received, access will be removed for any unconfirmed users.	**Priority**	3
	Responsible Officer	ICT Systems Support Team Leader
	Timescale	Implemented

Agreed Action 4.3 - Servitor		
A standard template has been adopted to record the checks and actions carried out as	**Priority**	3

result. Three reminders will be sent to managers and if a response is not received, access will be removed for any unconfirmed users.	**Responsible Officer**	ICT Systems Support Team Leader
	Timescale	Implemented

Agreed Action 4.4 - FMS		
A standard template has been adopted to record the checks and actions carried out as result. Three reminders will be sent to managers and if a response is not received, access will be removed for any unconfirmed users.	**Priority**	3
	Responsible Officer	ICT Systems Support Team Leader
	Timescale	Implemented

Audit Opinions and Priorities for Actions

Audit Opinions
Audit work is based on sampling transactions to test the operation of systems. It cannot guarantee the elimination of fraud or error. Our opinion is based on the risks we identify at the time of the audit. Our overall audit opinion is based on 5 grades of opinion, as set out below.

Opinion	Assessment of internal control
High Assurance	Overall, very good management of risk. An effective control environment appears to be in operation.
Substantial Assurance	Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified.
Reasonable Assurance	Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made.
Limited Assurance	Overall, poor management of risk with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation.
No Assurance	Overall, there is a fundamental failure in control and risks are not being effectively managed. A number of key areas require substantial improvement to protect the system from error and abuse.

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.

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.