APPENDIX 4

AUDIT REPORTS WITH MODERATE OR LOW LEVEL OF ASSURANCE ISSUED QUARTER 4 2018/19

System Ownership and Management – 31 January 2019

1 **Introduction**

1.1 In accordance with the Audit Plan for 2018/19 an audit review of System Ownership and Management was completed in December 2018 by Andy Shade from Internal Audit's IT audit contractor, TIAA. This report presents the findings and conclusions drawn from the audit for information and action where appropriate.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and co-operation received during the audit.

2 **Background**

2.1 This audit was undertaken to ensure that Council systems are managed appropriately and controlled through the use of a designated system owner/ owners.

3 **Scope and Objectives of the Audit**

3.1 The objective of the report was to ensure that adequate processes are in place around the management and ownership of key Council systems and that system owner's roles and responsibilities are appropriately defined and documented.

3.2 Testing was performed to confirm that controls identified have operated as expected with documentary evidence being obtained where possible, although some reliance has had to be placed on verbal discussions with relevant staff.

3.3 The audit was designed to assess and provide assurance on the risks pertaining to the following key areas:

- Documentation of system owner roles and responsibilities
- Management of superuser/ admin activity
- System support arrangements
- Ownership of third party relationships
- Access control processes and procedures.

4 **Findings**

4.1 **Recommendations from Previous Report**

4.1.1 This section is not applicable as this is the first audit of this area.

4.2 **Policies & Procedures**

4.2.1 The ICT policies and procedures relevant to systems ownership and management were identified and obtained during the review. These were used in the process of reviewing the suitability of the controls in operation at the Council.

4.2.2 The policies and documents identified as being of particular relevance in this review are the; 'Information Security and Conduct Policy', 'Software Policy' and 'System Owners Guidance'.

4.2.3 An understanding of the Council's approach to systems management was obtained through discussion with ICT and business management and review of available process documentation.

4.3 **Documentation of system owner roles and responsibilities**

4.3.1 ICT are responsible for ensuring that each information system has a nominated system owner. The roles and responsibilities of systems owners are defined as part of the 'Information Security and Conduct Policy'.

4.3.2 ICT Services maintains a list of all the Council's key applications and the relevant system owners. ICT Services carries out an annual review to ensure that the information is up-to-date and that system owners are aware of their roles and responsibilities.

4.3.3 A sample of Council systems was selected as the basis for testing in consultation with management. These were Acolaid, ActiveH and Idox. System management and user administration processes were discussed with the relevant administrators for each system to gain an understanding of the control environment.

4.4 **Access control processes and procedures**

4.4.1 User set up, change and removal processes were walked through and key application security controls including authentication controls and password settings were obtained and reviewed for each of the systems tested.

4.4.2 It was found that, for the systems tested, requests for account set up, change and removal were completed through the use of an email from the staff member's manager rather than through the use of a standardised user request form.

4.4.3 Rather than specifying the access individuals require in the system, or specifying a particular role based permission, managers will often nominate an existing member of staff to base the new starters' permissions on. It was also noted that there is no explicit requirement that a record of user requests is retained.

Risk

Staff may be granted access above the needs of their role or able to retain a level of access they no longer require.

Recommendation

Management should introduce a requirement that standardised user request forms are completed for key Council systems when requesting new users or changes to existing users access permissions. Forms should be retained to provide assurance that appropriate access rights have been granted to users according to their job role.

4.4.4 It was noted that regular leaver reporting is generated by HR in line with the Council's payroll runs and distributed to ICT and system owners on a monthly basis to ensure relevant teams are aware of leavers.

4.4.5 Leaver data was obtained and reviewed against application user accounts to ensure no leavers retained active accounts. This identified 16 leavers with active Acolaid accounts and 3 leavers with active Idox accounts.

Risk

There could be unauthorised access to systems and data via the misuse of active leaver accounts.

Recommendation

The accounts in question should be reviewed and all leaver accounts should be disabled.

4.4.6 System user accounts were reviewed for default supplier accounts, test accounts and the use of generic accounts with the potential risk of being shared between multiple users. This highlighted the existence of 8 Idox accounts that appear to be generic, shared or test accounts.

Risk

The use of shared / generic accounts removes accountability for activities performed and increases the risk of unauthorised access to the application.
Recommendation

The accounts should be reviewed and any generic accounts replaced with named individual accounts for those requiring access.

4.4.7 User account security settings including password parameters were obtained for each of the key applications and reviewed as part of the audit. This testing identified that, in general, passwords were sufficiently complex and included requirements for special characters and numerals, password length, password age, password length and password history.

4.4.8 It was confirmed that system support arrangements are in place for each of the systems tested. In the case of ActiveH the Systems and Support team perform a first line/ triage service raising ICT incidents or contacting the third party supplier where required, while the relevant systems support officer also acts in this role for the Acolaid and Idox systems.

4.5 **Management of superuser / admin activity**

4.5.1 Administrator and high level privilege accounts were obtained and reviewed with management for each of applications tested to confirm that accounts were appropriately restricted to authorised staff only. Accounts with the ability to create new users and/or reset the passwords of existing users were extracted and reviewed with management to verify these had been assigned to appropriate users only.

4.5.2 It was noted that, whilst the relevant administrators may perform some ad-hoc checking of accounts, there is no regularly scheduled and documented review of user account permissions performed for the systems tested.

4.5.3 A regularly scheduled exercise to review the validity of user permissions and accounts would help ensure that user's privileges within the application are appropriately restricted, and that any changes required as result of staff changing roles have been considered.

Risk

Staff have access to data/functions above and beyond that required for their job role, and/or may be able to "collect" systems access when changing roles.

Recommendation

A regular account review process should be introduced for all key Council systems. This should be performed at least annually and require team managers to confirm that users under their supervision have appropriate access rights within the application and that all leavers have been removed.

5 **Conclusions**

5.1 Although the audit did not highlight any urgent issues impacting materially on the Council's ability to achieve its objectives it did identify four Medium-rated issues which, if addressed, will improve the control environment to a worthwhile degree.

5.2 As a result, the findings are considered to give MODERATE assurance regarding the Council's system ownership and management risks

5.3 The assurance bands are shown below:

Level of Assurance	Definition
Substantial Assurance	There is a sound system of control in place and compliance with the key controls.
Moderate Assurance	Whilst the system of control is broadly satisfactory, some controls are weak or non-existent and there is non-compliance with several controls.
Limited Assurance	The system of control is generally weak and there is non-compliance with controls that do exist.

6 **Management Action**

6.1 The recommendations arising above are reproduced in the Action Plan for management attention.