INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	ICT Business Applications - MIS ActiveH Housing and Property Management
TO:	Head of Housing and Property Services Housing Strategy & Development Manager	**DATE:**	10 August 2016
C.C.	Chief Executive Deputy Chief Executive Head of Finance Business Support Manager Service Improvement Manager		

1 Introduction

1.1 In accordance with the Audit Plan for 2016/17, an examination of the above subject area has been completed recently and this report is intended to present the findings and conclusions for information and action where appropriate.

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

2 Background

2.1 The Active H integrated housing management system is supplied by MIS. The majority of system users are within Housing & Property Services, although there are a number of ancillary users spread across other services throughout the council. Contractors managed by Housing and Property Services also have limited access to the system.

2.2 The application software is mainly accessed via desktop work stations, although a facility to connect via mobile devices has been implemented for Building Surveyors in the Asset Management Division. The application is hosted on the Council's virtual server estate and run on a back-end SQL Server relational database management system.

3 Scope and Objectives of the Audit

3.1 The audit examination was undertaken for the purpose of reporting a level of assurance on the adequacy of IT application controls in respect of the MIS ActiveH business system to secure the confidentiality, integrity and availability of data stored and processed in support of the housing and property management functions of the Council.

3.2 The examination focused upon the key IT application controls in place to ensure that:

- an appropriate level of control is maintained over input, processing and output to ensure completeness and accuracy of data ;
- a complete audit trail is maintained which allows an item to be traced from input through to its final resting place, and the final result broken down into its constituent parts; and
- controls are in place to ensure observance of relevant corporate policies avoid and to avoid breaches of any law, statutory, regulatory or contractual obligations.

3.3 The controls were ascertained, evaluated and tested by reference to the CIPFA Systems-Based Audit Matrices (specifically the Application Controls module and those aspects of the Change Control module pertaining to deployment of application updates). The key areas focused upon were:

- compliance
- logical security controls
- user security controls
- input and processing
- audit trail
- change control (application release).

3.4 As part of the examination, an analytical review of user, role and functional security levels was attempted. In the event, however, the scope of testing achievable was restricted by data audit software failure linked to the recent updating of the virtual desktop environment.

3.4 The findings are based on discussions with relevant staff in Housing and Property Services and ICT Services, supported as appropriate by documentary evidence, system displays and data analytics. The principal staff contacts were:

Anna Monkton, Business Administration Manager
Daniel Leach, System and Performance Improvement Officer
Richard Southey, Application Support Analyst.

4 Findings

4.1 Recommendations from previous report

4.1.1 The current position in respect of the recommendations from the audit reported in December 2012 is as follows (overleaf):

Recommendation	Management Response	Current Status
1 The need for classifying the data held within Active H should be reviewed, with steps taken accordingly depending on the outcome of this review.	Agreed. The need for classifying data held within Active H will be reviewed.	The importance of this recommendation has diminished as a result of subsequent revision of the Data Handling Policy. Discussed further under 4.2.2. (Compliance) below.
2 Password control should be strengthened by amending parameters within the system. Minimum length requirement should be set to eight characters and frequency of password changes should be reduced to every 90 days in line with other systems in use.	Testing will be performed to ensure that these suggested changes will not invalidate users' current passwords, and lock them out of the system.	Implemented – now set to 90 days.
3 The 'account lockout threshold' within the security parameters should be amended to lock users out after a specific number of unsuccessful attempts.	This will be covered as part of the testing detailed above.	Implemented – now set to five attempts.
4 The use of the audit logging function should be reviewed to ensure that the tables being logged are of use to management and the system administrators.	Agreed. The use of the audit logging function will be reviewed accordingly.	Implemented – a review was undertaken with advice from ICT Services. The decision was taken to maintain the scope of audit logging in force.

4.1.2 There were three further recommendations of a highly elaborate and technical nature emanating of a specialist review of database management controls. While it is not seen as appropriate to reproduce them in detail here, it is confirmed from subsequent documented feedback that these recommendations were duly implemented.

4.2 Compliance

4.2.1 Appropriate regulatory controls were found to be in place to ensure that the application meets applicable statutory requirements and its use complies with relevant legislation and internal policies. The following key controls have been verified from testing:

- Applicable purposes of processing data have been notified as required under the Data Protection Act 1998;
- Appropriate system documentation is in evidence;

- The system ownership provisions of the corporate Information Security and Conduct Policy have been observed for the application;
- There are appropriate contractual provisions to ensure that the application is updated with all relevant legislation.

4.2.2 The previous recommendation on classification of data processed was made in the context of a Data Handling Policy that has subsequently been revised. The present Policy places is emphasis more on applying data classification to 'document marking' rather than internal data processing. The key expectation is that the data is processed in a secure environment befitting the highest sensitivity classification that would apply (in this case 'RESTRICTED' given presence of personal and commercially sensitive data).

4.2.3 In this context, the system environment is regarded as appropriately secure.

4.2.4 While the commonly accepted maximum number of system administrators in any business application is three, the nature of the ActiveH with its wide range of functional modules combined with devolved responsibilities for system management clearly justifies a greater number.

4.2.5 Users can be assigned one of three base security levels: User, Super User and Administrator. Datasets extracted from the back-end database showed nineteen users set up at Administrator level, broken down as follows:

	Number of 'Administrator' users
Generic	3
Housing and Property Services:	
Business Administration Team	4
Service Improvement Team	3
Building Surveying and Construction	1
Income Recovery	1
ICT Services – Application Support Team	7

4.2.6 Two of the generic IDs users were original set-up and maintenance users from when the system was first installed and have to be preserved, while the third is required to maintain the website interface. Access to the passwords for these is appropriately secured.

4.2.7 The structural profile of the Housing and Property Services users reflects respective team roles in key areas such as user management, parameter maintenance and functional development (including connection of mobile devices). The only exception is the user in Income Recovery which has been queried (the member of staff concerned is known to have had user management responsibility prior to a recent reorganisation in Housing and Property Services).

4.2.8 While requirement to have continuous technical support capacity available for the system is acknowledged, whether this justifies so many Administrators in ICT Application Support is seen as questionable at least (the same observation was made in a recent review of the Acolaid Planning, Building Control and Land Charges).

4.2.9 While the perceived risk involved is not seen as so significant as to warrant a formal recommendation, the matter was raised with the Business Administration Manager during the audit and subsequently reviewed in consultation with ICT Services. As a result, two users were had their access level changed to operational user and a further two temporarily disabled.

4.3 Logical Security Controls

4.3.1 Within the confines of the inherent design of the application, the logical controls meet the expected standards of security by:

- assignment of unique user identifiers and passwords with access to create, change or disable users restricted to system administrators;
- enforced disciplines for secure passwords;
- limits to failed login attempts before user lock-out;
- user role structure enabling access permissions to be tailored to users' responsibilities;
- only system administrators can access system audit tools.

4.4 User Security Controls

4.4.1 Appropriate controls are in place to ensure that:

- operational users are made aware of their responsibilities when using the application (via sign-up to the information Security and Conduct Policy and on-line ICT induction);
- access rights are promptly removed for employees who leave the Authority or change duties.

4.4.2 The Business Administration Team is responsible for user management for the ActiveH system, which represents a separate of duties from normal day-to-day operations. Awareness of changes affecting user access needs relies on a combination of notification by the respective users' line managers and periodic leavers' reports. At the time the previous audit, an annual e-mail canvass of users had been performed, although this process has lapsed following the subsequent organisational changes in Housing and Property Services.

4.4.3 The outcomes from the limited analysis and inter-matching on extracts from user and group permission tables confirmed, with only isolated exceptions, that all current ActiveH users are valid with no indication of permissions at significant variance to their respective roles (subject to the observations from the 'Adminstrators' test – 4.2. above). The exceptions related five former temporary employees and one former contractor which have now been disabled.

4.4.4 The exercise has demonstrated that current arrangements for notification and acting on staff changes are substantially effective in their own right, subject to the potential for isolated cases of users to 'slip through the net'.

4.4.5 Given this, the reintroduction of annual canvassing of users is suggested as an informal advisory for consideration.

4.5 Input and Processing

4.5.1 Input processes are substantially regulated by a combination of automatically generated values, mandatory entries, in-built format validations and a considerable array of parameter tables. The parameters are made up primarily of code tables which tend to remain fixed after they have been introduced.

4.5.2 The key parameter tables identified that are comparatively fluid are those for property rents and contract schedules of rates. These can only be changed in ActiveH by system administrators, in practice designated officers in the Service Improvement Team which makes the process independent of users involved in day-to-day operational input. It was confirmed from enquiries that appropriate checks are in place when these parameters are updated.

4.5.3 All relevant documents supporting inputs are scanned into an electronic document management repository and are accessible by link from the respective ActiveH records.

4.5.4 In the ActiveH system environment, the processing controls are essentially tied to input validation. Routine processes operate automatically without the need for any operator intervention and do not require any form of scheduling to synchronise with input activities.

4.5.5 Financial data transfer to and from the application is verified through established core financial control procedures operated by Housing Services and Finance.

4.6 Audit Trail

4.6.1 It was re-verified that audit logging is active in the ActiveH system that the audit trail displays all requisite information to enable error tracking, suspect inputs, etc. It should be noted, however, that the operational inputs leave transparent trails that can be generally accessed by record view and management reports.

4.6.2 The audit logging settings were confirmed as representing the scope of auditing determined at the management review that had been undertaken in response to the previous audit recommendation.

4.7 Change Control (Application Release)

4.7.1 At the time of the audit, a system upgrade was underway and it had been envisaged that a review of the release control process would be based on this project while it progressed. This could not be accomplished since the testing phase was still in progress at the conclusion of the audit, therefore the examination followed the usual process based on historic documentation from the most recent completed system release implementation.

4.7.2 Reference was made to available documentation regarding an upgrade implemented in 2014. This re-confirmed for the most part that the application release process conforms with the corporate ICT Change Management Policy and standard Business Application Release procedures.

4.7.3 The only element that could not be specifically tested here specifically was the sign-off for live implementation since the relevant Software Acceptance Certificate could not be located (it was advised that the document had been held in the former Help Desk system which had since been replaced without the document being migrated).

4.7.4 In view of this, some additional work has been approved to review the upgrade project in progress at the time of this report on a consultancy basis. Any findings that may impact on the level of assurance will be reported separately.

5 Conclusions

5.1 Following our review we are able to give a SUBSTANTIAL degree of assurance that the controls are adequate to secure the said confidentiality, integrity and availability of the systems and related information assets.

5.2 Levels of assurance are applied based on the following bands:

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.

5.3 There are no recommendations arising from the examination.

Richard Barr
Audit and Risk Manager