INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	ICT Business Applications – Active H Integrated Housing Management System
TO:	Head of Housing & Property Services Head of Corporate & Community Services	**DATE:**	14 December 2012
C.C.	Chief Executive Head of Finance ICT Services Manager Business Manager		

1. Introduction

1.1 In accordance with the Audit Plan for 2012/13, an examination of the above subject area has been undertaken and this report presents the findings and conclusions drawn from the audit for information and action where appropriate. This topic was last audited in September 2007.

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 cooperation 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 other users throughout the council, notably within the Customer Service Centre. Some contractors also have limited access to the system.

2.2 The application software is used via networked desktop PCs to connect and interact with a back-end SQL Server relational database management system installed on the Windows server operating system. The database server is installed on the server named 'MAXSQL' that sits in the virtual server estate.

3. Scope and Objectives of Audit

3.1 The examination was undertaken to assess the adequacy of key controls in place for the applications supporting housing management to ensure the completeness, accuracy, security and effectiveness of data input, processing and output. These controls may be provided either by programming and configuration within the application systems or by manual controls exercised by users.

3.2 The review focused upon the key IT application controls based on the following system control objectives:

- 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.
- Arrangements exist for creating backup copies of data and programs, storing and retaining them securely, and recovering applications in the event of failure.
- Controls are in place to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

3.3 The audit approach used the Application Controls module of the CIPFA Matrices for Information Technology supplemented by adapted elements of the Change Control module. The expected controls under these matrices are categorised into the following areas:

(1) Compliance
(2) Logical security controls
(3) User security controls
(4) Parameter data
(5) Transaction input
(6) Data processing
(7) Output
(8) System availability
(9) Audit trail
(10) Change control – application release

3.4 The audit approach was to evaluate the controls by completion of an Internal Control Questionnaire and undertaking compliance testing where appropriate by applying the CIPFA Matrices model. This was performed through:

- consultation and discussion with appropriate members of Housing & Property Services staff and the relevant Application Support Analyst
- inspection and analysis of relevant documentation, system reports, displays, data exports, etc.

4. Findings

4.1 Compliance

4.1.1 This area of the review covers compliance controls to ensure that the application meets any regulatory and statutory requirements and its use complies with relevant internal policies.

4.1.2 The Council is registered to process person identifiable data as evidenced by the Data Protection registration document, registration number Z623925X. The main use of the system is covered under 'Purpose Three' (Property Management).

4.1.3 The use of Active H is subject to internal policies such as the corporate Information Security & Conduct Policy (ISCP) and relevant sub-policies. The ISCP tends to set out how individuals who manage or use the applications should act, rather than setting out requirements for the actual applications.

4.1.4 For example, access control, covered under Section 24 of the ISCP (Password & Logins) states that Employees and Members must adopt sound password practices, including complexity, regular changing etc, so unless the system constraints will not allow these things, it is up to the user to ensure that they comply with these requirements.

4.1.5 One of the relevant sub-policies is the Data Handling Policy. This covers, amongst other things, the requirement for all data held by the council to be classified. Upon discussion with the system owner and system administrators, it was identified that none of the relevant staff were aware of whether the data held on Active H had been classified in line with the policy.

Risk
Breach of internal policies.

Recommendation
The need for classifying the data held within Active H should be reviewed, with steps taken accordingly depending on the outcome of this review.

4.2 Logical Security Controls

4.2.1 Within the confines of the inherent design of the application, the logical controls meet the expected standards of security. Individual user accounts and passwords are set up, with access to create, amend and delete users being restricted to system administrators. The user accounts are assigned to one or more roles which are designed to allow access to specific functions and modules as considered necessary for the users to undertake their duties. The system will then only display the functions that the user has access to.

4.2.2 Whilst there is a level of control within the system to enforce some password discipline, such as minimum length, blocking the use of previously used passwords (last ten), prohibiting certain passwords (e.g. those that contain part of the username) and the frequency with which passwords should be changed, some of these are not as rigid as they could be.

4.2.3 Some controls cannot be enforced by the system, such as requiring a mix of different character types (i.e. alphanumeric and special characters), but other controls could be strengthened by changing parameters on the system. Current settings only require passwords to be a minimum of five characters and they only have to be changed every 120 days.

Risk
Unauthorised system access enabled by weak password control.

Recommendation
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.

4.2.4 It was also noted that the current settings do not enforce the locking out of user accounts should they fail to enter the correct password after a specific number of attempts.

Risk
Unauthorised system access enabled by weak password control.

Recommendation
The 'account lockout threshold' within the security parameters should be amended to lock users out after a specific number of unsuccessful attempts.

4.2.5 Control over access to the database and operating system has been examined by the IT Audit Partner. Three specific issues were highlighted which can be summarised as:

a) The purpose and origin of the instance-level 'administrator' account is unclear.

Risk
Unauthorised administrative access to all databases that are hosted on the SQL Server instance.

Recommendation
The purpose and origin of the instance-level 'administrator' should be ascertained. The privileges assigned to this account should subsequently be adjusted as appropriate.

b) A review of the logins assigned to the dbo_owner role has not recently been undertaken

Risk
Unauthorised administrative access to the database.

Recommendation
A review of the logins assigned to the dbo_owner role should be undertaken. Changes should subsequently be made as appropriate to ensure that only those with a genuine operational need retain this level of privilege and that the correct domain account for each Application Support user is used where administrative privileges are to be retained.

c) A review of the privileges and permissions assigned to users through the ActiveHGRP database role has not been undertaken.

Risk
Inappropriate access to privileges and permissions for the underlying database.

Recommendation
The privileges and permissions provided to the ActiveHGRP database role should be confirmed. The risk associated with users being inappropriately assigned to this role should subsequently be assessed. If the risk is deemed sufficient to require review, the domain and SQL Server-level accounts assigned to the role should be reviewed to ensure that only current members of staff and other authorised accounts remain assigned to the role. The review should include membership of all domain groups assigned to the role, including through nested domain groups such as WARWICKDC\engineers, which is assigned to the WARWICKDC\Housing ActiveH Access domain group.

Full technical details of these issues can be found in Appendix B

4.3 User Security Controls

4.3.1 Users of Active H are made aware of their responsibilities when using the application via sign-up to the Information Security and Conduct Policy and upon completion of their on-line ICT induction.

4.3.2 The system administrator questioned (Senior Finance Officer (SFO)) highlighted that he is provided with lists of leavers via the Rents & Finance Manager. Users identified via these lists will have their access privileges disabled, although they are not deleted from the system as this may affect historic transactions that remain on the system.

4.3.3 An annual review of access is also performed by the SFO, with emails being sent to each department to ascertain if users within the department are still require the access permissions which they have been granted.

4.3.4 Details of the current users and their access permissions were reviewed and questions were raised with the SFO with regards to some of the current access privileges. He highlighted that some of the roles assigned were historic and access needs would be confirmed again as part of the next annual review.

4.4 Parameter Data

4.4.1 The nature of the application means that there are no known parameters that require periodic manual updating. Amendments to parameters such as the repairs authorisation limits are ad-hoc and require relevant access levels which were found to be appropriately controlled.

4.5 Transaction Input and Data Processing

4.5.1 There majority of input onto the system is manual, and is largely controlled via the use of drop-down lists, mandatory entries, default values etc. On the whole, there is no supporting documentation for this input with the exception of Home Choice applications which are input onto the lettings module. The forms are marked with the relevant, system generated, application number to confirm that they have been entered.

4.5.2 The only other form of input relates to cash and benefit postings to the rents module. Files are received from the relevant systems (PARIS and Civica Open Revenues) and are uploaded onto Active H. Reconciliations are performed between the amounts uploaded onto Active H and the corresponding import files to ensure that all relevant amounts have been input appropriately.

4.5.3 On the whole, this processing does not require any coordination with other system inputs. However, when debit raises are being undertaken, an email will be sent round to Housing & Property Services staff to ask them to come out of the rent accounts to ensure that the process can operate smoothly.

4.5.4 However, if an account has been left open, the system will identify which accounts had not been processed, and the process can then be rerun for the selected accounts.

4.6 Output

4.6.1 Output from the system is generally management information reports that are individually generated and, as such, there is no requirement for controls to be in place. Some letters are generated by the system in relation to housing applications but again, these are individually generated and are collected directly by the staff member who has generated them.

4.7 System Availability

4.7.1 System availability is assured by centralised database management, system back-up and test restore operations overseen by the ICT Infrastructure Team. An audit of ICT Backup Strategy, Processes and Procedures has recently been undertaken by our contracted IT Audit partner, so the processes were not examined as part of this audit.

4.8 Audit Trail

4.8.1 The purpose of an audit trail is to ensure that:

- sources of transactions or amendments to standing data are traceable
- output data is verifiable
- inter-system data flows can be reconciled to substantiate financial ledgers
- the guilty party in the event of a fraud or irregularity can be identified.

4.8.2 Within Active H, amendments to rent accounts are logged by default. System administrators can also select whether other tables are to be logged or not. However, the Application Support Analyst advised that system performance is affected by use of the facility so the logging of additional tables was not generally undertaken.

4.8.3 Upon review it was identified that five additional tables are being logged. However, the system administrator questioned did not know how to find the audit logs and advised that they were not reviewed.

Risk
Sources and instigators of suspect transactions or unauthorised data changes cannot be identified.

Recommendation
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.

4.9 Change Control – Application Release

4.9.1 Updates to the business application system should follow a course of action prescribed within the Council's (ICT) Change Management Policy and the Business Application Release processes contained therein.

4.9.2 Paperwork for the latest upgrade was found to be in place and had been completed appropriately, with checklists being completed and the tests performed having been signed off on behalf of the system owner.

4.9.3 Detailed testing documentation was provided by the System & Performance Improvement Officer who advised that, in general, the testing had worked well, although one subsequent issue had been noted due to the tests undertaken by staff on one specific module. However, she advised that this had been rectified quickly.

5. Summary & Conclusion

5.1 Following our review, we are able to give a MODERATE degree of assurance that the systems and controls in place surrounding the use of the Active H Integrated Housing Management System are appropriate and are working effectively.

5.2 Issues were identified relating to the classification of data held within the system, the password strength and user lock out settings that are currently in place, database access restrictions and the use of the audit logging function.

6. Management Action

6.1 Recommendations arising above are reproduced in the attached Action Plan (Appendix A) for management attention.

Richard Barr
Audit and Risk Manager

Appendix A

Action Plan

Internal (ICT Business Applications) Audit of Active H Integrated Housing Management System – December 2012

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer	Management Response	Target Date
4.1.5	The need for classifying the data held within Active H should be reviewed, with steps taken accordingly depending on the outcome of this review.	Breach of internal policies.	Medium	Business Manager	Agreed. The need for classifying data held within Active H will be reviewed.	April 2013
4.2.3	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.	Unauthorised system access enabled by weak password control.	Low	Application Support Analyst & Senior Finance Officer	Testing will be performed to ensure that these suggested changes will not invalidate users' current passwords, and lock them out of the system.	April 2013
4.2.4	The 'account lockout threshold' within the security parameters should be amended to lock users out after a specific number of unsuccessful attempts.	Unauthorised system access enabled by weak password control.	Low	Application Support Analyst & Senior Finance Officer	This will be covered as part of the testing detailed above.	April 2013
4.2.5 (a)	The purpose and origin of the instance-level 'administrator' should be ascertained. The privileges assigned to this account should subsequently be adjusted as appropriate.	Unauthorised administrative access to all databases that are hosted on the SQL Server instance.	Medium	Database Administrator	The administrator account has been disabled.	Complete

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer	Management Response	Target Date
4.2.5 (b)	A review of the logins assigned to the dbo_owner role should be undertaken. Changes should subsequently be made as appropriate to ensure that only those with a genuine operational need retain this level of privilege and that the correct domain account for each Application Support user is used where administrative privileges are to be retained.	Unauthorised administrative access to the database.	Medium	Database Administrator	A review has been performed and three logins have been removed (mis_service, ActiveHUser and cpritchard). It was confirmed that the other members are necessary for administering the application.	Complete
4.2.5 (c)	The privileges and permissions provided to the ActiveHGRP database role should be confirmed. The risk associated with users being inappropriately assigned to this role should subsequently be assessed. If the risk is deemed sufficient to require review, the domain and SQL Server-level accounts assigned to the role should be reviewed to ensure that only current members of staff and other authorised accounts remain assigned to the role. The review should include membership of all domain groups assigned to the role, including through nested domain groups such as WARWICKDC\engineers, which is assigned to the WARWICKDC\Housing ActiveH Access domain group.	Inappropriate access to privileges and permissions for the underlying database.	Medium	Application Support Manager	An assessment of the risk has been completed and it has been deemed sufficient to require a review of the accounts assigned to the role, including the nested domain groups. This review has commenced, but will take some time due to the number of accounts involved.	End of February 2013

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer	Management Response	Target Date
4.8.3	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.	Sources and instigators of suspect transactions or unauthorised data changes cannot be identified.	Low	Business Manager	Agreed. The use of the audit logging function will be reviewed accordingly.	April 2013

* Risk Ratings are defined as follows:

Low	-	Minimal adverse impact on achievement of the Authority's objectives if not adequately addressed.
Medium	-	Moderate adverse impact on achievement of the Authority's objectives if not adequately addressed.
High	-	Requires urgent attention with major adverse impact on achievement of Authority's objectives if not adequately addressed.

Appendix B

Technical Details Relating to Findings at 4.2.5

a) The purpose and origin of the instance-level 'administrator' account is unclear.

Privileges for administering a database in SQL Server can be assigned at instance or database level. Where privileges are assigned at instance level to the SYSADMIN fixed server role, the assigned administrators are able to administer every database on the instance. The ActiveH database is the only vendor-supported database on the instance and the vendor can therefore be expected to be assigned to the SYSADMIN role for support purposes. This is provided via the WARWICKDC\mis-se domain account. An additional login called 'Administrator' is also in place, however, and the Database Administrator was not aware of the origin of this account or its purpose.

b) A review of the logins assigned to the dbo_owner role has not recently been undertaken.

The dbo_owner fixed database role for a database allows any users assigned to that role to administer all objects within that database. Access to this role should therefore be tightly controlled. Discussions with the Database Administrator and an initial inspection of the user logins assigned to this role confirmed some potential issues with the current assignment of users:

- ActiveHUser and mis_service. These logins are at SQL Server-level and are likely to have been created by the vendor. The purpose of these logins is unclear as the vendor also has a domain account (WARWICKDC\mis-se) that is assigned privileges at instance level;
- WARWICKDC\david.adcock. This login applies to a business analyst within Application Support who needs access to the database in order to create bespoke reports. This should not require database owner privileges though. The account is also the domain user account for this users as opposed to his administration account for this user. Each member of ICT who has any administrative responsibilities has a separate account at domain level that they should use when undertaking administrative tasks.
- WARWICKDC\richard.southey is a member of Application Support. This account is also the regular domain user account as opposed to the administrative domain account for this user.
- WARWICKDC\cpritchard is the head of application support. It is understood that this login is no longer needed and can be removed. The account is also the user account as opposed to the administrative account for this user.

c) A review of the privileges and permissions assigned to users through the ActiveHGRP database role has not been undertaken.

The ActiveH application is unusual in that the application does not connect to the underlying SQL Server database via a single defined account. Instead, the application front end connects each user to the database via their individual domain log on. This is achieved by assigning each user's domain account to the ActiveHGRP database role. Discussions with the Database Administrator and an initial inspection of user allocation confirmed that:

- It is unclear what privileges and permissions are provided to users by their membership of the role;
- The method of assigning logins to the role is complex, with users assigned to the role via membership of domain groups that are nested within another domain group; and
- A review has not been undertaken to confirm whether all users assigned to the role still require that access.