INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	MIS Housing and Corporate Property (ActiveH) Application
TO:	Deputy Chief Executive (AJ)	**DATE:**	4 February 2021
C.C.	Chief Executive Head of Finance Head of Assets Head of Housing Services Head of ICT Services Application Support Team Leader Business Development & Change Manager Compliance Manager Portfolio Holder (Cllr Day)		

---

1 Introduction

1.1 In accordance with the Audit Plan for 2020/21 an audit review of the Council's MIS Housing and Corporate Property Application (ActiveH) was completed in December 2020. 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 The MIS ActiveH Housing Management Application is used by the Council to manage its housing and corporate property assets. The majority of system users are within Housing Services and Assets, although there are a number of ancillary users spread across other services throughout the Council. Contractors undertaking work on the Council's properties also have limited access to the system.

3 Scope and Objectives of the Audit

3.1 The objective of the report was to ensure the security, integrity and availability of the Council's ActiveH Application

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

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

- Application Management and Governance
- System Security
- Data Input and Output
- Change Controls
- Interface Controls and Processing
- System Resilience and Recovery
- Support Arrangements.

4 Findings

4.1 Recommendations from Previous Report

4.1.1 This section is not applicable as the previous audit report from August 2016 did not include any recommendations.

4.2 Application Management and Governance

4.2.1 It was identified that a Data Protection Impact Assessment (DPIA) has not yet been conducted for Active H although the need to conduct the assessment has been acknowledged by senior management.

4.2.2 The Data Protection Act 2018 requires that a DPIA be conducted for all systems that process personal data. The process is required to be carried out as part of the implementation of new systems or where a significant change to an existing system has taken place.

Risk

There may be an increased risk of non-compliance with the Data Protection Act 2018 if a DPIA has not been undertaken.

Recommendation

Council management to work with relevant Information Governance colleagues to complete a DPIA on the MIS ActiveH Application in a timely manner.

4.2.3 There are staff in place whose role is to act as system administrator for the application. The Business Development & Change Manager in Housing Services is the Information Risk Owner for the application.

4.2.4 We have noted that there are training processes embedded within the department and that the training is supported by relevant training guidance, a sample of which was obtained and reviewed as part of the audit fieldwork. The guidance is made available within a library available on the network and there is work underway to look into the feasibility of implementing an interactive Intranet training service. Should further training support be requested by users, a request for closer support can be made.

4.2.5 The audit has noted that the training that is provided is not routinely being recorded within a training register or other suitable recordkeeping mechanism.

Advisory

Consideration to be given to keeping a training log or register to demonstrate the nature of the training being provided, to whom and when. Such records may help inform future training needs based on existing knowledge.

4.3 **System Security**

4.3.1 Requests for new accounts and changes to existing accounts are made via email from a recognised staff member. The requests include the level of access required for the user.

4.3.2 Users are allocated their own username and temporary password when the account is first set up. The application automatically marks the temporary password as requiring a change when the password is first used.

4.3.3 Should a user forget their password, a temporary password is assigned to the account to allow the user to log in, whereupon the same automated password change process causes the password to be changed to make it unique to the user when the account is used again. We have also noted that password complexity has been enabled to the extent permitted by the application's design.

4.3.4 Periodic reviews of user accounts take place with the reviews being assigned to local staff within the departments that have access to the application. The results of the reviews are saved to a central network location.

4.3.5 It was noted that the Council's internal auditors have access profiles for the application that are always available for their use as they act for others in the Council on a periodic basis and have regular need to refer to the data processed by the application for other reasons. However, it is noted that the access profiles are not read-only profiles. Hence, there is a need to ensure that the auditor access profiles are revised so that they have no more than read-only access to the data.

Risk

Inappropriate access controls may increase the risk of inadvertent or unauthorised changes to the data processed by the Application. This could result in non-compliance with Data Protection Act 2018 requirements.

Recommendation

The accounts assigned to the internal auditors should be reviewed such that they are assigned read-only access at the most.

4.4 Data Input and Output

4.4.1 A review of a sample of screens that are used to process data within the application was undertaken. It was identified that there is widespread use of drop down lists where specific options can be selected. It was also noted that available options in other drop down lists for other fields are modified depending on options selected in other fields. For example, if a property that has no bedrooms is selected, options related to bedrooms are disabled so that there can be no interaction with them.

4.4.2 The use of drop down lists and the fact that the behaviour of other fields changes depending on what is selected elsewhere helps to ensure consistency of input, which, in turn, helps increase the integrity of data being reported in management information that is made available on a routine or ad-hoc basis.

4.4.3 The review also identified that there is a range of 'error trap' functionality that displays error messages when attempting to save data that is not accurate or formatted correctly. This is supported by red dots with exclamation marks inside them that appear when badly formatted data has been entered. Hovering over the dots reveals a 'tooltip' that explains the reason for the dot appearing.

4.4.4 If an attempt to save the data is made, the error message described above will be displayed. The red dots are used as a warning to the user that something they have input is unlikely to be accurate. If the errors are cleared before being saved, the red dots disappear.

4.4.5 The application also makes use of mandatory fields and colours those fields so that it is clear to the user that some form of entry is required. Mandatory fields are pink. It is not possible to save forms where incomplete pink fields are present. Yellow is used for fields that are for information only (although this is customizable). An example of this might be a field displaying the full address of the asset being displayed at that time.

4.4.6 The application also includes a number of tabs within the screens that can be used to design bespoke processing screens. The forms are called User Design Elements (UDE) and are labelled 'Additional Details'. The Council uses these screens for additional, bespoke data input, although it was noted that validation of the input in these UDEs has not been enabled. As an example, a successful attempt was made to enter a date in the year 3000, which was not flagged as an error in the relevant UDE field.

4.4.7 This is due to the fact that the design of the forms and the fields used also requires validation routines to be assigned to each field to help prevent inaccurate or incorrectly-formatted data from being entered. The review noted that there is a separate screen available that can be used to configure appropriate validation routines for the field concerned. An example of this could be to create validation to prevent birth dates forward of today and possibly any dates that fall outside of a specific time frame prior to today, should the age of a tenant be relevant to the scenario in question.

Risk

Inconsistent data entry may increase the risk of inaccurate management information and possible service disruptions.

Recommendation

All of the UDE screens/ forms should be reviewed in order to apply appropriate validation to the relevant fields.

4.4.8 The Ripplestone report management system is used for all relevant reports, which manages the creation, distribution and storage of reports built using Crystal. MIS incorporates its own reporting tool, although it is not used to the same degree.

4.5 Change Controls

4.5.1 There is a formal process for accepting a change and authorising ICT to promote a change into the live system. The process includes a range of authority options:

- Agreed to promote having completed all testing to the satisfaction of the authorised person;
- Agreed to promote without testing and confirm that the business takes responsibility for the decision;
- Withdraw the change completely and give a reason why.

4.5.2 Part of this process, for upgrades and complex development changes, includes a summary test spreadsheet showing the final testing results for all areas being tested in order to demonstrate the rationale behind the authority to proceed with promoting the upgrade into the Live environment.

4.6 Interface Controls and Processing

4.6.1 There are manual interface processes in place for posting entries between the finance system and ActiveH. The processes are documented as user guides. The processes include the manual selection of input files created by other systems and moving the 'used' files into folders so that the new input file that is created for the next processing run does not conflict with the one previously used.

4.7 System Resilience and Recovery

4.7.1 There are alerts in place that are part of the VMWare environment that the application and database are hosted within. The alerts are designed to provide warnings on infrastructure issues that may require attention. Such issues include capacity warnings where disk space may be low. The alerts are recorded within the IT Service Desk system for resolution.

4.7.2 ActiveH is hosted on two main environments - maxapp2 (the application) and maxsql2 (the database). These are both hosted as Windows virtual machines and are included in the corporate backup processes.

4.7.3 Every three days, the latest disk backup is copied offsite to the Town hall disk backup server. This process also has a number of previous restore points retained covering the last 60 days or so.

4.7.4 Every seven days, the latest disk backup is copied to tape and stored at the Town Hall. The Town Hall is a few streets away from the main Council office.

4.7.5 A documented Housing Services crisis plan is in place, dated November 2019. The Council has also documented a corporate Business Continuity Plan, which the crisis plan is linked to. However, the document was last reviewed in 2014. Hence, a further review is required to ensure that it remains fit for purpose.

4.7.6 However, a focussed Business Continuity audit is planned for 2021/22 (having been deferred from the current year's audit plan) and this issue will be covered as part of that audit. Hence, no recommendation is being raised in this report.

4.8 Support Arrangements

4.8.1 There is a general satisfaction with the system and there has been a recent major upgrade to keep it aligned to business needs and for support purposes.

4.8.2 The support relationship is managed by the business area although ICT also log support calls with MIS's helpdesk if the issues are something that the Council is unable to resolve. MIS is the supplier; however, they do not manage the application or database servers as the infrastructure is entirely managed by the Council's ICT Service. If it becomes necessary, MIS can connect remotely to the Council's infrastructure should more direct support be required.

4.8.3 Such access needs to be requested by either MIS or the business as the account they use for this is disabled by default. Disabling accounts until required in this way is accepted good practice for security reasons.

4.8.4 ActiveH upgrades are managed entirely in house; with MIS supplying the software and associated instructions.

5 Conclusions

5.1 The audit did not highlight any urgent issues materially impacting the Council's ability to achieve its objectives. A result, the findings are considered to give SUBSTANTIAL assurance around the management of database security risks.

5.2 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.

Level of Assurance	Definition
Limited Assurance	The system of control is generally weak and there is non-compliance with controls that do exist.

5.3 However, a number of issues were identified:

- A Data Protection Impact Assessment (DPIA) has not been completed for the system
- The access profile for Internal Audit staff is not restricted to read only access
- User Design Elements (UDEs) currently allow incorrectly formatted data to be entered.

5.4 A further 'issue' was also identified where an advisory note has been reported. In this instance, no formal recommendation is thought to be warranted as there is no risk if the action is not taken. If the change is made, however, the existing control framework will be enhanced:

- Consideration to be given to keeping a training log or register to demonstrate the nature of the training being provided, to whom and when. Such records may help inform future training needs based on existing knowledge.

6 Management Action

6.1 The 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 Audit of the MIS Housing and Corporate Property (ActiveH) Application – February 2021

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.2.2	Council management to work with relevant Information Governance colleagues to complete a DPIA on the MIS ActiveH Application in a timely manner.	There may be an increased risk of non-compliance with the Data Protection Act 2018 if a DPIA has not been undertaken.	Medium	Business Development & Change Manager (Housing Services – System Owner)	Agreed. A Data Protection Information Assessment DPIA for the ActiveH application will be developed and signed off by the Council's Information Governance Manager.	30 April 2021
4.3.5	The accounts assigned to the internal auditors should be reviewed such that they are assigned read-only access at the most.	Inappropriate access controls may increase the risk of inadvertent or unauthorised changes to the data processed by the Application. This could result in non-compliance with Data Protection Act 2018 requirements.	Low	Business Development & Change Manager (Housing Services – System Owner)	Agreed. The level of access permission to be adjusted to read only access. If the system does not facilitate the creation of Read Only accounts, accounts used for auditing purposes could be disabled or removed until they are required.	19 February 2021

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.4.7	All of the UDE screens/ forms should be reviewed in order to apply appropriate validation to the relevant fields.	Inconsistent data entry may increase the risk of inaccurate management information and possible service disruptions.	Medium	Business Development & Change Manager (Housing Services – System Owner)	Agreed. To review existing UDE screens and forms, apply the appropriate validations and conditions to those still in use. This would have to be a joint undertaking between ICT, to support the changes, and the service area to identify which business items are crucial and must be updated.	30 April 2021

* Risk Ratings are defined as follows:

High Risk: Issue of significant importance requiring urgent attention.
Medium Risk: Issue of moderate importance requiring prompt attention.
Low Risk: Issue of minor importance requiring attention.