INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	ICT Business Applications - IDOX Acolaid Planning, Building Control and Land Charges
TO:	Development Manager	**DATE:**	30 June 2016
C.C.	Chief Executive Deputy Chief Executive (BH) Head of Development Services Head of Consortium (Building Control) Head of Finance ICT Application Support 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, in any recommendations made. My thanks are extended to all concerned for the help and co-operation received during the audit.

2 Background

2.1 The Acolaid system is a suite of modules used for the management of services provided by Development Services including planning applications, land charges and building regulations. The system was implemented as part of the development of planning and regulatory services on-line (PARSOL) under the Implementing Electronic Government (IEG) programme of the early 2000s.

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 is run on the corporate virtual server estate.

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 IDOX Acolaid business system to secure the confidentiality, integrity and availability of data stored and processed in support of the provision of the planning, building control and land charges 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 on were:

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

3.4 Although most of the evaluation was in the form of overview and update following on from the findings of the previous audit (January 2012), outstanding issues concerning user access controls were considered in greater depth including analysis of user permission data.

3.5 Controls relating to the IDOX electronic document management system attached to the Acolaid system were not covered within the scope of this audit.

4 Findings

4.1 Recommendations from previous report

4.1.1 Several of the recommendations from the previous report (January 2012) were addressed to the Development Manager as designated system owner. It should be noted that a change of Development Manager postholder has since occurred.

4.1.2 The current position in respect of the recommendations is as follows:

Recommendation	Management Response	Current Status
1 The number of Acolaid licences held should be ascertained with a review being subsequently performed to ensure that this is still relevant to the needs of the Council.	The former Development Manager advised that the software supplier would be consulted on this and a review undertaken.	The current Development Manager was unaware of any contact made, but expressed his intention to investigate the potential of cost savings on user licences covering both Acolaid and the EDRMS.
2 The password expiry setting should be activated.	After some queries, the former Development Manager advised that the setting had been activated.	A re-check showed that the setting is no longer active. It is not clear whether it had been activated and subsequently de-activated and, if so, whether this was by a conscious system ownership decision. The issue is re-considered under Section 4.3 (Logical Access Controls) below.
3 A review of system access permissions should be performed to ensure that all users have relevant access privileges and that obsolete and duplicate accounts (and groups) are deleted.	The former Development Manager advised that a review had been undertaken and that user accounts for leavers had been disabled. Review of existing user account privileges would follow.	The current Development Manager could not recall whether the review of existing user account privileges had been undertaken. A further review has been scoped into the audit and the outcomes are considered in Section 4.2 below.
4 The membership of the db_owners fixed database role should be confirmed for all databases under the live instance for Acolaid. Once confirmed, the administrative requirements of the Application Support Team at database level should be confirmed with a view to restricting access in line with operational needs.	The Database Administrator had advised that the Application Support staff had been removed from ‘db_owners’ fixed database role.	This arose from a specialist review of the back-end database performed by an external expert which has not been re-performed in this audit.

Recommendation	Management Response	Current Status
5 A regular (annual) review should be performed of all users with system access to ensure that the privileges remain relevant.	This had been agreed by the former Development Manager.	The audit found no formal process for annual review. It was advised the reliance was placed on the relevant divisions of Development Services and other service areas to notify changes affecting Acolaid users. This issue is considered further (see Section 4.4 below)
6 Options suggested by the Application Support Analyst with regards to enabling specific users to be identified on the audit trail (either via integration with Active Directory or by setting users up on the database) should be investigated and adopted if they are considered to be relevant and proportionate.	The Application Support Manager advised that the system supplier would be contacted to determine the feasibility of this.	This was implemented by integration with Active Directory so that the audit log now identifies the network logon user that performed each action.

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; and
- The system ownership provisions of the corporate Information Security and Conduct Policy have been observed for the application.

4.2.2 The Application Register records the Development Manager as sole designated system owner. Some concern about this was expressed in discussion given that it implies certain responsibilities extending to the Building Control function over which he has no managerial control. It was advised informally that the possibility of a split or shared role with the Head of Consortium could be pursued (this would have to be raised with the ICT Application Support Manager).

4.2.3 As an accredited PARSOL system, Acolaid is maintained under agreement with updates as necessary to support implementation of changes to planning laws, land charges regulations, building regulations and other relevant legislation.

4.2.4 Two issues emerged under the 'compliance' theme, both of which had been raised in the previous audit report. At that time, there was no internal knowledge of how many concurrent user licences were in force and, therefore, it could not be gauged whether the Council was receiving appropriate value for money in respect of the annual system maintenance charges (see Section 4.1, Recommendation 1 above).

4.2.5 It is noted that this information started to appear on the maintenance invoices from 2013 onwards, although no management review of licensing requirements has been undertaken to date. In discussion, the Development Manager advised that a review of licensing for the IDOX document management system has been planned and it is envisaged that this will extend to Acolaid.

4.2.6 For the key modules of Development Management and Building Control, the number of licences represent an almost exact one-to-one ratio to the number of operational staff in post at the time of the audit (in the case of the former, Planning Policy staff have been included in the equation). This does not include ICT Application Support and casual users in other service areas.

4.2.7 From the maintenance rates charged, the number of licences would have to be reduced by a substantial proportion to achieve significant cost savings. As a model example it was calculated that a 25 per cent reduction in the number of licences across all applicable modules would achieve an annual saving of around £6,000.

4.2.8 In view of the above, it is not deemed appropriate to make a formal recommendation on this matter.

4.2.9 The other issue to re-emerge is connected with the outstanding recommendation for review of system access permissions (see Section 4.1, Recommendation 3 above). This had stemmed from an observation that sixteen users had accounts that gave them effective system administration permissions over the entire application.

4.2.10 A more in-depth analysis has shown the number now to be twenty-two, broken down by function as follows:

	Number of users with full system administration rights
Development Management	6
Building Control	7
GIS	3
ICT Application Support	6

4.2.11 Interestingly, the ICT Application Support category includes a generic user 'AppSupport' that has never been used since the system was installed.

4.2.12 It had been argued at the time of the previous audit that giving this blanket access was the only way to some allow users to access certain tables, but this view is not supported by the system manual which indicates that such access needs can normally be met by assigning specific lower level 'security objects' directly to users. In fact, the picture to emerge of user and user group security settings comes across as messy, inconsistent and with unnecessary duplication, even allowing for the inherently granular nature of the security system. The observations here demonstrate a lack of proper understanding of the way in which the Acolaid security system works and possibly some misconceptions over terminology.

4.2.13 While the commonly accepted maximum number of system administrators in any business application is three, the devolved nature of operations using Acolaid may justify a higher number, but no more than seven (two each in Development Management and Building Control, and a maximum of three in ICT Support).

Risk
Potential abuse or misuse of the system by users with inappropriate access levels (deliberate or inadvertent).

Recommendations

(1) A core of no more than seven system administrators should be designated for the Acolaid system.

(2) Appropriate training should be provided on the Acolaid security system for the designated administrators.

(3) A review of all current system access permissions should be commissioned and access levels restored to those appropriate to the roles of the respective users.

4.3 Logical Access Controls

4.3.1 Within the confines of the inherent design of the application, the logical security controls were found to substantially meet the following expected standards:

- assignment of unique user identifiers and passwords with access to create, change or disable users restricted to designated system administrators;
- parameters to enforce disciplines for user passwords available and set at an appropriately secure level;
- limits to failed login attempts before user lock-out;
- user role structure enabling access permissions to be tailored to users' responsibilities;
- user profile data tables are protected including encryption of passwords.

4.3.2 The only noticeable exception to the above is the matter of password expiry raised in the previous audit (see Section 4.1, Recommendation 2 above). Historically, the password expiry setting had not been enabled so that users were never forced to change their Acolaid sign-on passwords.

4.3.3 Whether the expiry setting had been enabled for a time in accordance with the previous recommendation is not known, but its current status at the time of the audit was found to be disabled.

4.3.4 Although this represents a departure from the expected standards contained in the Information Security Policy, there are other factors that can be argued to challenge the need for forcing Acolaid password changes in practical terms. The key factors are:

- inherent information risks – the information processed is essentially public domain material and does not in itself generate financial transactions;
- network security layer – access to the Acolaid application requires user credentials permitting logging into the corporate network and Acolaid client assignment;
- identification of users performing actions in the Acolaid audit log – the users are identified by linkage to Windows Active Directory which means that it is the user ID of the person logged into the desktop from which action is performed that is captured irrespective of whether the same person is signed in to Acolaid.

4.3.5 This was explained in discussion with the Development Manager who formed the opinion that the level of risk involved did not warrant pressing the matter of Acolaid password expiry. This view is respected.

4.3.6 Inter-matching and analysis was used on extracts from user and group permission tables in an attempt to cut through the granularity of access set-up and gauge whether current users' privileges appropriately reflect their responsibilities.

4.3.7 Except for the issue of the widespread assignment of system administration privileges already discussed, the exercise generally confirmed this to be the case subject to certain observations.

- The BCOfficers group and a small number of users are assigned 'Create' permissions at <Application> level, giving the applicable users permissions to create records in areas outside their remit;
- A number of security objects have been needlessly assigned to users individually that replicate permissions already established by group membership (relates specifically to Building Control).

4.3.8 This is seen as a further symptom of the overly widespread assignment of system administration privileges and lack of proper understanding of the Acolaid security system among the system administrators already discussed.

Risk
Potential abuse or misuse of the system by users with inappropriate access levels (deliberate or inadvertent).

Recommendation
The security object assigning 'Create' permission at <Application> level should be removed from the BCOfficers group and from the individual users identified (details supplied separately).

Risk
System response may be impaired by unnecessary security object assignments to individual users.

Recommendation
The security objects assigned individually to users in the BCOfficers group should be checked and those replicating the group security objects removed.

4.4 User Security Controls

4.4.1 Operational users are made aware of their responsibilities when using the application (including a sign-up to the Information Security and Conduct Policy and on-line ICT induction).

4.4.2 Testing in the previous audit showed that processes in place were not entirely effective in ensuring that responsible system administrators were notified of and acted upon users that had left the Council or had changed duties so as to longer require access. The recommendation arising was for an annual review of all users.

4.4.3 There is still no formal process for this in evidence and results from testing showed that current arrangements for communicating and acting on staff changes affecting user rights are still not working effectively. Of the 106 'live' users at the time of the audit, 28 were confirmed as redundant (these have been referred for disabling in the system).

4.4.4 A number of these were found to have left up to three years previously and there were also users found to have been dormant for several years (shown by the last login date field in the extracted user table).

4.4.5 From a discussion with the designated Application Support Officer for Acolaid, two potential solutions emerged:

- exploitation of the linkage between Acolaid and Active Directory to generate e-mail alerts when leavers with Acolaid client assignment have their network access rights removed;
- generation of a report of 'live' users showing last login dates thus enabling identification of dormant user accounts as part of a periodic (e.g. annual) review.

Risk
Unauthorised access and potential misuse of the system.

Recommendations

(1) The feasibility of e-mail alerts to the system administrator on removal of leavers with Acolaid access from the corporate network should be explored.

(2) An annual review of active Acolaid user accounts should be performed supported by a report showing last login dates.

4.5 **Input and Processing**

4.5.1 The system in effect is a general record of approaches and applications received in relation to the various services provided by Development Services as opposed to a transactional based system. Cases are dealt with on an individual basis and processing is real-time with validation where applicable effected at the time of input (e.g. through drop-down code tables).

4.5.2 Input is either manual, based on documentation received directly from applicants, callers, etc., or electronic if an application has been received via the Planning Portal or Submit-a-Plan.

4.5.3 Data received via the portal is imported onto the system via the XML gateway, with a case being created on Acolaid and relevant fields being automatically populated. Financial data (e.g. fees charged and paid) are recorded for case progression purposes only and the system does not generate financial transactions.

4.5.4 Due to the nature of the system, i.e. being essentially a case record 'library', there is very little separation of duties built into the system with no specific input requiring independent authorisation. This is not considered to be a weakness, as controls over the processes exist outside of the computer system.

4.6 **Audit Trail**

4.6.1 It was re-verified that audit logging is active in the Acolaid system and that the audit trail displays all requisite information to enable error tracking, suspect inputs, etc. As stated above, the originating user of each action is now identified by the Active Directory login name.

4.7 **Change Control (Application Release)**

4.7.1 By reference to documentation relating to the latest system release, it was re-confirmed that the application release process conforms with the corporate ICT Change Management Policy and standard Business Application Release procedures.

5 Conclusions

5.1 While issues relating to user permission settings have been discussed at some length, they do not in themselves represent an inordinate threat to the confidentiality, integrity and availability of the information assets. Considering the whole scheme of controls over the application, the findings support a SUBSTANTIAL level of assurance that the controls are adequate to secure the said confidentiality, integrity and availability.

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.
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 attached Action Plan (Appendix A) for management attention.

Richard Barr
Audit and Risk Manager

Appendix A

Action Plan

Internal Audit of ICT Business Applications – Acolaid Planning, Building Control and Land Charges – June 2016

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.2.13 (1)	A core of no more than seven system administrators should be designated for the Acolaid system.	Potential abuse or misuse of the system by users with inappropriate access levels (deliberate or inadvertent)	Medium	Development Manager		
4.2.13 (2)	Appropriate training should be provided on the Acolaid security system for the designated administrators.		Medium	Development Manager		
4.2.13 (3)	A review of all current system access permissions should be commissioned and access levels restored to those appropriate to the roles of the respective users.		Medium	Development Manager		
4.3.8 (1)	The security object assigning 'Create' permission at <Application> level should be removed from the BCOfficers group and the individual users identified (details supplied separately).		Low	Development Manager (to assign to authorised system administrator)		

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.3.8 (2)	The security objects assigned individually to users in the BCOfficers group should be checked and those replicating the group security objects removed.	System response may be impaired by unnecessary security object assignments to individual users.	Low	Senior Building Control Officer (DT)		
4.4.5 (1)	The feasibility of e-mail alerts to the system administrator on removal of leavers with Acolaid access from the corporate network should be explored.	Unauthorised access and potential misuse of the system.	Low	Development Manager (in consultation with Application Support Manager)		
4.4.5 (2)	An annual review of active Acolaid user accounts should be performed supported by a report showing last login dates.		Low	Development Manager (in consultation with Application Support Manager)		

* 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.