WARWICK DISTRICT COUNCIL

INTERNAL AUDIT REPORT

FROM: Audit and Risk Manager

TO: Senior Management Team
ICT Services Manager

C.C. ICT Applications Support Manager
Technical Support Manager

SUBJECT: Document Management Systems

DATE: 27 July 2012

---

1. INTRODUCTION

1.1. In accordance with the Audit Plan for 2012/13, 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. SCOPE AND OBJECTIVES OF AUDIT

2.1 Electronic document management (EDM) facilities are utilised by several applications providing the means for electronically stored documents to be accessed via the application and, in some cases, to form part of automated workflows. The examination focused upon strategic provisions governing the approach to developing EDM corporately and management of their operation and associated risks.

2.2 The evaluation was based on the following control objectives:

- A defined strategy for the provision of electronic document management facilities is in place;
- Information classifications have been assigned to all data sets stored on document management systems; and
- Operational risks relating to the provision and use of electronic document management facilities have been assessed and controls reflect an agreed approach to managing those risks.

2.3 The audit approach aimed to identify and profile all active EDM systems operated by the Council through:

- consultation and discussion with key officers associated with managing and supporting the EDM systems;

§ examination of documentary evidence in respect of strategies, policies, risk assessments, assignment of responsibilities, business cases, benefit realisation, data classification and access control as applicable.

3. FINDINGS

3.1 Overview of Strategy and Systems

3.1.1 The original development programme for EDM was focused on the design and build of a single solution expected to integrate with all major back-office systems and support service delivery workflow. Ultimately, for various reasons, this had to be abandoned and a more devolved approach to EDM has since emerged.

3.1.2 This devolved approach can be seen as emanating from the Document Management Solutions (DMS) Programme which was approved by the Executive in October 2008, by which time the Housing Benefits function was already in the process of implementing the EDM and workflow solution which had already been available as a module of the existing business application.

3.1.3 The review leading up to the seeking of approval for the DMS Programme recognised that a lack of defined measurable benefits had left no real basis for proving return on the DMS investment to date. With substantial amounts already expended and committed, cost reduction was to prove a major driver for the new approach and the evidence seen indicates that this has been achieved.

3.1.4 Initially, the DMS Programme was subject to both senior management review and Member scrutiny until being effectively closed in June 2009. Implementations of EDM have continued since, although in a climate of changed priorities as manifested in the Fit for the Future Programme.

3.1.5 In the course or the examination, nine major active document management 'repositories' have been identified and profiled, seven of which directly support business application systems. Categorised into their respective relationship with the DMS Programme, these are:

pre-dating the DMS Programme in development/implementation:

§ Civica OpenRevenues – document image processing (DIP) and workflow module for housing benefits (subsequently rolled out to council tax and business rates replacing Fortis system previously used)

§ Chipside – DIP attached to parking enforcement application (standard system chosen by Warwickshire County Council for all Warwickshire districts)

§ 'WDCShare' – a general network resource traditionally used for electronic file sharing (later also the initial repository for documents created using the corporate 'scan and store' facilities);

specifically provided for in the DMS Programme;

- IDOX – replaced Trinity EDRMS as DIP and workflow tool for Planning and Land Charges
- Microsoft Office Sharepoint Server (MOSS) – serves as Intranet platform and as Council-wide collaborative tool and shared document store (current application is limited and the DMS Programme envisaged a wider roll-out to Service Areas);

implemented after closure of the DMS Programme (June 2009):

- TOTAL – DIP module of Financial Management System used for creditor invoices (replaces Fortis system previously used)
- Housing Management - documents scanned through corporate 'scan and store' facilities and linked to the related ActiveH asset records (replaces Fortis system previously used). A parallel system for Housing Strategy is approaching implementation at the time of the audit, also using 'scan and store' and linking to housing application records on ActiveH.
- Environmental Services, Licensing and Private Sector Housing – documents scanned through corporate 'scan and store' facilities and moved to designated file system folders to link to the related APP Civica application records.
- Fortis SE – recently acquired for storing employee documents relating to payroll processing (migrated from MOSS which in turn replaced an older version of Fortis no longer supported).

3.1.6 The current ICT Strategy (2011 to 2015) refers generally to the development and promotion of "paper-light" environments continuing the shift from paper to electronic storage and sharing of documents, but does not go into detail on the technology platform(s) this will be based on. The DMS Programme advocated the roll-out of MOSS as a key solution for corporate document and records management, although subsequent developments showed limitations to MOSS as a document management platform supporting key business processes. MOSS has not been used for Housing Strategy 'scan and store', as originally envisaged in the DMS Programme, and the Payroll DMS has migrated away from MOSS.

3.1.7 From the outset of the audit, it was clear that DMS is not supported by any information classification framework and there is no evidence of operational risks specific to document management facilities having been assessed. For evaluation purposes, the key risks were defined as:

- poor value for money and operational inefficiency;
- inability to differentiate between the value of documents within document management facilities and across document management systems;

§ Unauthorised access to electronically-stored documentation;

§ Inability of application users to undertake workflow and other tasks involving electronically-stored documents.

3.1.8 With this above in mind, the profile undertaken on each of the systems listed above focused (where applicable) on:

§ implementation background (e.g. defined business case, evaluation of options, costs/funding, etc.)

§ hardware set-up (scanning and storing);

§ controls over operational processes (scanning, referencing and file movement as applicable);

§ security of document repositories against unauthorised access.

3.1.9 The findings are discussed below in the context of these themes.

3.2. <u>Implementation Background</u>

3.2.1 This was looked at only in respect of those systems post-dating the DMS Programme in their implementation. These are distinguished by fact that no major costs were incurred in implementing them (not counting internal staff time involved which is probably considerable but has not been measured).

3.2.2 Fortis SE is the only software product solution that has been specially purchased for document management since the closure of the DMS Programme. The Total Portal for creditor invoice DIP was already licensed to the Council while the Housing and Environmental etc. systems adopted the corporate 'scan and store' facilities and file transfer processes were designed internally to attach the captured document images to the applicable back-office system records. This was because either no suitable third party solution was available or the cost of such a solution was found to be prohibitive.

3.3 <u>Hardware Set-Up</u>

3.3.1 For each of the profiled systems, the facilities for scanning and referencing documents fall into one of four basic scenarios:

§ dedicated scanner(s) attached to desktop console PC (Civica Open Revenues, Chipside, IDOX and Fortis SE);

§ scan on Council general purpose mopier with special configuration and reference via PC with software client installed (Total Portal)

§ scan on any Council general purpose mopier and move captured images through referencing process linked to back-office system (Housing, Environmental, etc).

§ scan on any Council general purpose mopier without any linking with back-office systems (WDCShare).

3.3.2 The first two scenarios represent the best controlled physical and logical environment giving greater efficiency and assurance of document integrity throughout and after the capture process. In the third and fourth scenarios, the captured files are first stored in unsecured network folders and require manual intervention to ensure that valuable and confidential material is moved to an appropriately secure repository.

3.4 Operational Processes

3.4.1 For the systems in the first of the above set-up scenarios, the scanning and referencing processes are activated and driven by modules of the back-office systems to which they relate. They require password protected user login to access. For IDOX and OpenRevenues, the facility includes in-built pick lists and record searches to help ensure correct referencing and workflow generation.

3.4.2 All systems in this group are supported by documented operational procedures and, with one exception, functionally integrated with the respective back-office systems. The exception is Fortis SE which, while supporting payroll operation, operates independently with no interface with the human resources management system.

3.4.3 Scanning to Total uses a mopier in the Document Management Centre requiring entry of a PIN on the machine to activate a special configuration to direct scanned documents to the requisite server location where they can be retrieved in the Total Portal. Access to the Portal requires password protected login.

3.4.4 The remaining profiled systems use WDCShare as a temporary repository and require service-based staff to perform file transfer operations in association with the back-office systems (where applicable). Compared to the systems in the first two of the aforementioned scenarios, this process appears relatively convoluted and involves use of Windows Explorer functions. While documented procedures have been produced for the Environmental, etc. file transfer and linkage with the back-office records, the same cannot be said for Housing, although it is reported that the process was incorporated in Moodle training.

Risk
Improper knowledge of correct procedures for transferring and linking scanned documents to the ActiveH housing management system may result in disruption of the process and possible loss of or unauthorised access to their content.

Recommendation
Procedures for transferring and linking scanned documents to the ActiveH housing management and application records should be documented.

3.4.5 A key issue with this temporary repository is that it has no default security leaving the documents, invariably containing personal data (some of it sensitive), accessible to virtually all Council staff to read, move or delete at will. This would not be an issue if the file transfer was always performed immediately after scanning, but this has proved not to be the case.

3.4.6 There is known to be a backlog of scanned housing tenancy documents waiting to be transferred at the time of the audit and some Environmental Health documents were found in the WDCShare folders that were several months old. This is seen as an exacerbation of a wider long-standing issue with WDCShare which discussed further under the 'repository security' theme below.

3.5 Security of Document Repositories

3.5.1 The devolved approach to DMS has inevitably brought with it a wide distribution of document repositories. In most cases, the permanent repositories sit on the application or database servers deployed for the back-office systems through which the documents are retrieved. This makes control of access to the documents intertwined with control over access to their respective applications (examined under separate audit assignment).

3.5.2 In most of the profiled systems, the network locations of the repositories are locked down through Active Directory settings to prevent 'back door' access through Windows navigation tools. This has been proved in test attempts to connect to the servers and their contents.

3.5.3 An exception was, however, revealed from discussions with ICT Application Support regarding creditor voices in Total. At the time of the examination, it was admitted that current default settings render the documents open to any staff who have a mind to navigate to the network location. A task had been set up to lock down the applicable folders, but with relatively low priority attached.

3.5.4 Although this represents a potentially significant vulnerability, there are some mitigating factors including:

- access would require a concerted navigation operation with knowledge of the server name;
- in a feature common to most of the profiled systems, automated sub-folder and file naming uses random alphabetic and numeric character strings making location of specific records via the 'back door' very difficult.

Risk
Important financial records could be lost through wilful malicious destruction.

Recommendation
Access restrictions should be placed on the network folders area holding creditor invoice document images linked to Total.

3.5.5 Attention now turns WDCShare as both a general file sharing facility and a temporary repository for documents captured through the corporate 'scan and store' facility. While some content is work group based and restricted, the vast bulk is made up of unsecured folders and files which continue to proliferate unchecked despite occasional purges in the past. This is substantially the result of folders and files being placed there and then forgotten about.

3.5.6 Particular alarming is the fact that some of this open is personal data. In a brief trawl through, examples were seen of:

- correspondence identifying details of complainants and the nature of their complaints;
- lists and correspondence showing names and addresses of community alarm subscribers;
- performance appraisals documentation relating to former staff;
- employment documentation re new appointee;
- risk assessment of Supported Housing client;
- housing application documentation;
- tenant rent balances and arrears recovery status;
- listings of housing benefit postings to tenant rent accounts showing names and addresses;
- contract tender documentation including pricing schedules.

3.5.6 The wide accessibility of this personal data is tantamount to unauthorised disclosure in breach of the Data Protection Act 1998. It is also strongly suspected that personal data content present has been held beyond the duration necessary to fulfil the legitimate purposes, also in breach of the Act.

3.5.7 It is known at the time of this report that an exercise to purge WDCShare content is under way. However, the there is the deeper issue of failure to manage WDCShare content on a corporate basis that will only perpetuate the related information risks if not addressed. The situation is seen as particularly symptomatic of a lack of:

- any enforced structure in the creation of WDCShare content;
- defined file management responsibilities;
- policies on WDCShare content based on information classification;
- awareness of the insecure nature of WDCShare and data privacy implications.

3.5.8 The DMS Programme had looked to MOSS to meet the need for effective records management, although a contingent measure of reverting back to Meridio (a Microsoft product component of the former EDRMS) was also envisaged. What does not come out clearly is whether or not MOSS (or Meridio) was expected to completely supersede WDCShare.

3.5.9 There is clearly scope for some of the information resources in WDCShare to be migrated to MOSS and, at the time of the audit, a business case for MOSS upgrade to facilitate expanded application is being prepared. For the purpose of this report, however, it has to be assumed the WDCShare will remain in some form for the foreseeable future. On that basis, management is asked to address the need to establish a corporate framework that will ensure efficient, effective and legally compliant use of the facility. As a key principle, the overriding control responsibility under such a framework must rest with the respective content authors and their line managers.

3.5.10 As part of the framework, the following approach is suggested:

- implement clear policies on use of WDCShare to include required security measures and retention limits in line with information classifications under the Data Handling Policy;
- establish an enforced Service Area based main folder structure under which employees can only create folders and files within their own respective Service Area domains;
- revive the network of Service Area Information Champions (originally formed in the wake of the Freedom of Information Act 2000) with a brief to regularly monitor WDCShare content relating to their own respective Service Areas in addition to their traditional roles.

Risk

The Council may be held in breach of data privacy legislation with consequent financial penalties and damaging publicity.

Recommendations

(1) All unsecured content of WDCShare should be deleted or moved to secure repositories.

(2) The feasibility of restricting access to the 'scan and store' repositories in WDCShare should be investigated.

(3) A framework for managing the content of WDCShare should be developed and implemented based on clear policies and assignment of responsibilities.

(4) An alternative document management and sharing platform to replace WDCShare should be investigated.

4. CONCLUSIONS

4.1 The picture emerging on DMS is one of contrasts. The change of approach as manifest in the DMS Programme has led to devolved systems in place that appear to function well, but does not leave any clear picture on return on investment or any clear assessment of the operational risks arising.

4.2 At the time of the audit, the development of DMS supporting the major back-office functions and related business applications is nearing completion, effectively leaving residual corporate document management needs to be addressed. From the profiling exercise performed as part of the audit, the systems generally show sound operational controls in place ensuring the completeness and integrity of the documents on their journey from paper to electronic destination. With one exception, the final repositories were shown to be subject to appropriate network controls to prevent unauthorised access without impeding legitimate retrieval.

4.3 Conversely, the systems that rely on the corporate 'scan and store' facilities have shown data security issues that do not affect those using third party solutions.

4.4 The unmanaged proliferation of content in WDCShare, combined with delays in transfer of scanned documents in Housing, have resulted in material that should have been kept confidential effectively open for all Council staff to see (and manipulate), including personal data. The past occasional purges of content have not addressed the root cause – lack of a managed approach to controlling content in the first place. Most of the recommendations are focused on remedying this.

4.5 In view of the above issues, the findings are considered as giving MODERATE assurance that appropriate controls are in place to effectively manage the risks that could prevent the electronic document management framework and systems from achieving their objectives.

6. MANAGEMENT ACTION

6.1 Recommendations to address the issues raised are reproduced in the appended Action Plan for management response.

Richard Barr
Audit and Risk Manager