BENEFITS OF USING AN INFORMATION SYSTEM TO: CAPTURE, SECURE & PROVIDE ACCESS TO ELECTRONIC DOCUMENTS

The increasing difference in cost between maintaining paper and electronic records and the requirement to access information quickly make it in every organisation's interest to maximise its use of electronic records and minimise the use of paper[1].

In the past the organisation's network drive was one of the main repositories for electronic records. However, as the use of information systems, such as the Electronic Document and Records Management System (eDRMS) has increased, organisation's have been forced to consider the differences between these two repositories and the benefits, or otherwise, in providing security of and access to electronic documents.

USE OF NETWORK OR SHARED DRIVE STRUCTURES

The nature in which shared drives have evolved and the traditional approach of using the folder hierarchy in network drives provides limited flexibility in establishing appropriate and differing levels of access to electronic documents within different folders, based on different organisational workgroups. The complexities with implementing an information security and access model within a network drive based on the 'need to know' principle[2], as commonly used in information systems such as eDRMS, can lead to ineffective security of an organisation's information.

Shared drives have often evolved informally with little planning or structure. As a result, directory folders and documents may be poorly organised and titled. In an environment where records are supposed to be shared with a number of users, this lack of rigour will inevitably cause difficulty in locating, retrieving and using information and in managing versions. It also makes it difficult to assign security restrictions to certain parts of the business that may be more sensitive. [3]

SOME COMMON DRAWBACKS WITH USING NETWORK OR SHARE DRIVE STRUCTURES [4]

- The complexity of applying differing access restrictions based on different workgroups may result in staff getting access to information which they are not authorised to access and conversely not getting access to information they are authorised to access.
- Governance is not readily or easily applied because folders are easy to add and may grow exponentially without controls at various levels in the hierarchy.
- Often no contextual links between documents relating to the same business activity, and limited capture of metadata to support electronic documents.
- Difficulty finding and retrieving information that is known to exist, because of the relatively uncontrolled structures in a network drive.
- Documents are difficult to authenticate, and may therefore not provide reliable evidence, due to the fact that they are relatively easy to alter, move, and delete (intentionally or unintentionally), with limited audit trails left to identify who had access and who made what changes.

Phone 0438 275 751 | Email info@irisconsulting.net.au
www.irisconsulting.net.au

USE OF INFORMATION SYSTEMS SUCH AS AN EDRMS

In information systems such as the eDRMS, using a security and access model based on a 'Workgroup' approach, provides more flexibility and authorised access to information via the principle that access will be set at **'Open Access' by Default and 'Restricted by Exception'**. This approach is not easily and efficiently replicated in a network drive.

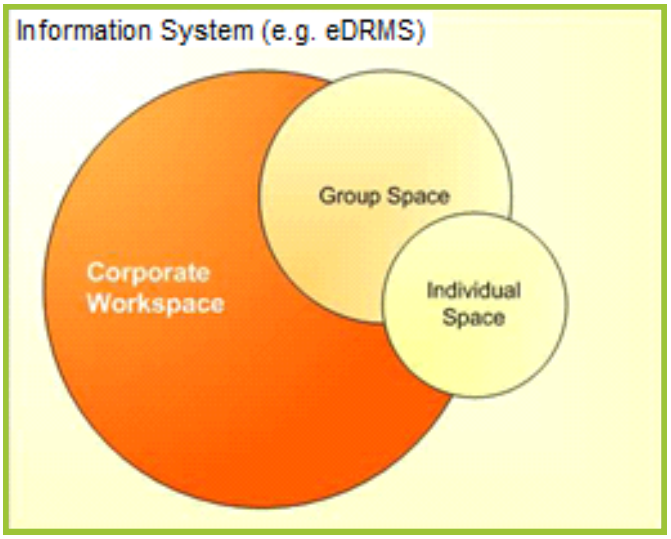
Benefits of implementing an EDRMS[5]

- Provides a secure and systematic central store in which to manage unstructured data such as emails, documents and spreadsheets, instead of uncontrolled shared drives, email folders or network drives.
- Provides greater security and access control features and audit trails to reduce the risk of corporate information being inappropriately accessed, altered, lost or deleted.
- Reduces legal liability exposure by the ability to prove the integrity of information used as evidence in any legal proceeding.
- Ability to integrate with other business systems (for example, case management systems) and collaborative work systems to access related information, which also enables improved information/ records capture through automation.
- Contextual links between related documents and records through use of electronic files or containers.
- Enable staff to view, read or share information simultaneously from their desktops, enabling sharing and reuse of information across workgroups.
- Quicker and more convenient discovery and access to information, previously spread across several repositories, which includes in support of discovery orders.
- Potential improvements in decision-making through access to the latest, accurate and most comprehensive information.

APPLYING A WORKGROUP SECURITY MODEL IN AN eDRMS

The workgroup approach used in information systems makes it easier to develop security classifications using the 'need to know' principle, which is based on the fundamental rule that security should be established according to a person's legitimate need to access information to carry out their duties.

Workgroups may be constructed when a person has a legitimate need to access and/or share certain types of information, which others may not have a legitimate need to know to undertake their work. A typical workgroup approach to implementing information security is illustrated in the diagram below.



WORKSPACES WITHIN AN INFORMATION SYSTEM

Corporate Workspace

Everyone belongs to by default, and where access is 'open' or unrestricted.

Workgroup Space

Space created to share information within a specific workgroup, restricting access only to that group:

- Examples of a workgroup are: a business unit, a group of Managers, or the Executive group.
- Each workgroup is established using a security classification model (internal or external).
- Access to information is restricted to only the nominated workgroup/s, it cannot be shared by everyone within the Corporate Workspace.

Individual Space

An area in which individuals may place information relating to their work environment, which is not accessible by others:

- Documents related to the individual, such as timesheets, leave forms, task lists etc can be stored here.
- This space MUST NOT be used to hold any corporate or workgroup documents as access is restricted to only the individual and the system administrator.

The design of a security model based on the work group approach needs to be well thought out to ensure that:

- Information which can and should be legitimately shared by 'All staff' is 'unclassified' and available for Open Access i.e. access is unrestricted.
- Establishment of workgroups is carefully considered, as too many workgroups may result in 'information silos' which prevent sharing of information.
- Workgroups are not used as a way to simply replicate the folders currently used in the share drive, as this will immediately create information silos.
- Creation of workgroups does not become excessive, as this increases the complexity of the security model and application of security classifications, resulting in a greater maintenance burden and costs to the organisation.

[1] Government Technology: *EDRM—the benefits.* Retrieved 21 February 2020 from http://www.governmenttechnology.co.uk/features/edrm-benefits
[2] Australian Government (2020) *Protective security policy framework*. Retrieved 21 February 2020 from https://www.protectivesecurity.gov.au/information/access-to-information/Pages/default.aspx
[3] Tasmanian Archive and Heritage Office. *Information management advice 41—Managing records on shared network drives*. Retrieved 21 February 2020 from https://www.informationstrategy.tas.gov.au/Records-Management-Principles/Document%20Library%20%20Tools/Advice%2041%20Managing%20Records%20on%20Shared%20Network%20Drives.pdf
[4] Queensland State Archives. *Managing Shared Drives* (2005). Retrieved on 6 May 2013 from http://bit.ly/13dJJte
[5] https://www.records.nsw.gov.au/recordkeeping/advice/faqs-edrms