

IMPROVING ELECTRONIC DOCUMENT MANAGEMENT – GUIDELINES FOR AUSTRALIAN GOVERNMENT AGENCIES

Excerpt:

Managing the System:

Successful implementation of electronic document management practices hinges on a number of operating issues. Issues revolve around the daily management of the electronic document management system and include:

- The provision and support for hardware, software and relevant upgrades
- Assignment of responsibility for technical performance evaluation and fine tuning of system
- On-going education for users
- Ensure reliable migration of electronic documents over successive generations of software and hardware—especially pertinent in the case of linked electronic documents and records
- Management of software upgrades and the conversion of data from one system to another can potentially corrupt documents w/compound documents at greatest risk
- Data management tools and techniques should be utilized in conjunction w/electronic document mgt. Data administrators have a responsibility to assist w/implementation
- Provide for security and privacy of the agency's data resources
- Backup across all platforms
- Maintaining details for systems backup and recovery
- Provide education for use of passwords and general security of machines and disks
- Carefully planned housekeeping issues: regularly reviewing electronic documents to ensure they are retained to meet business needs, avoid confusion about which is the current version and ensure that data storage capacity is efficiently used; Document deletion based on a consistent set of criteria.
- Data archiving to transfer data files offline to disk or tape storage and document name is removed from the directory. Responsibility exists to ensure that both short and long term storage of electronic docs is based on organizational business requirements.
- Review the system on a regular basis to ensure policies and practices are consistently applied across the organization
- Short term measure is to cope w/electronic docs and records stored on PC systems. Long term strategies revolve around designing and building electronic recordkeeping systems.

Australian government has recordkeeping professionals to analyze the business, technological and organizational nature and identify the recordkeeping requirements associated with that activity.

Government also engages a “review” team with a range of skills including records managers, librarians, archivists and information technologists to:

- Establish EDMS policy
- Identify all legislation that affects EDMS
- Expose shortfalls in EDMS policies, functions or practices
- Establish opportunities for new and improved record and doc mgmt policies, processes or systems

CONSIDERATIONS – when deciding on the scope and capacity of your EDMS information architecture:

- The network must be sufficiently robust in scope, size and capacity to accommodate large image files. Who should be connected, and where are they? What's the volume? Are there peaks? How is compression to be used?
- Actual scanning is a question of volume, flow, and peaks; of the decision on what has to be retained as an image; and of what data can be extracted at the point of scanning. Should documents be brought in singly or in batches?
- Image correction and improvement is a quality control feature that must be balanced against the need to save an image as is.
- Verification is a function of looking at a scanned image and its interpretation, and saying yes or no, keep or re-do.
- Indexing can be automatic or manual, but it is the vehicle by which the image will be retrieved. The format of the index database is also important.
- Storage is a question of physical device and file format, archiving and migration over time. Storage affects retrieval response time.
- Client functions include retrieval, annotation of the image, display options, and workflow.
- Server functions involve both network management and such items as workflow routing, and connections to other systems.
- Agencies should consider the "plug-and-play" features coming into the market.
- The system should provide a full range of security features so access can be restricted to the levels necessary.
- Preference should be given to software that is compatible with the agency's existing workstation software and network operating systems. Additional operating systems should not be required and user interfaces should be consistent with existing operating systems.
- The system should support the agency's existing database software to facilitate indexing and retrieval. Database software must be SQL compliant.
- The system should permit integration of multiple forms of storage so that response times, backup, and recovery requirements can be met. For example, the system should permit files that require more immediate response to be stored on hard disk or in memory and files with less critical response time requirements to be stored on microfiche, optical disk, or tape.
- The system should be scaleable. The ability to add additional functions, storage capacity, and image workstations, and the ability to distribute to other geographic locations should be provided.
- The system should support the storage and retrieval of documents from other computer applications without having to print and scan the documents. This can be accomplished by storing these documents in 'native' format (for example, a Word Perfect file would be stored in WP format; an ARC/info map in ARC/info format, etc.), by storing pointers to the documents, or by converting to another text format. These alternatives vary in cost and the amount of risk associated with converting documents when changing/upgrading various software packages and should be evaluated based on the program requirements for the agency.
- Systems should provide multiple options for indexing and retrieval of documents. Manual indexing, bar code recognition, and optical character recognition (OCR) should be supported.

NOTE: To view the entire report log onto: <http://www.defence.gov.au/imsc/edmsc/iedmpt1.htm>