



NATIONAL ARCHIVES OF AUSTRALIA

Implementing an EDRMS – Key Considerations

National Archives of Australia

V 1.0 2011



Australian Government
National Archives of Australia

© Commonwealth of Australia 2011

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the National Archives of Australia.

Requests and inquiries concerning reproduction and rights should be directed to the Government Information Management branch, National Archives of Australia, PO Box 7425, Canberra Mail Centre ACT 2610, Australia.

CONTENTS

Introduction	4
Electronic document and records management systems	5
What is an EDRMS?	5
Benefits of implementing an EDRMS	6
Use of EDRMS in Australian Government agencies	7
What an EDRMS cannot do	8
Improving digital information management without an EDRMS	9
Key considerations for implementing an EDRMS	10
Resource commitment	10
Required skills	10
Know your agency's requirements	11
Change management	12
Get the information management framework right	13
Integration with other systems	16
Migration from shared drives and legacy systems	17
Future and existing paper records	18
Security	19
Business continuity planning	19
Planning for long-term retention of digital records	20
System configuration	20
Training	21
Pilot before rollout	22
Choosing the right rollout option	22
Ongoing system operation and maintenance	23
References	24

INTRODUCTION

This document explains what electronic document and records management systems (EDRMS) are, what they can and cannot do, and what business benefits they can provide. It also highlights key issues that agencies will need to consider to achieve a successful EDRMS implementation which meets business needs and is accepted by its users.

The focus is on issues specific to EDRMS applications and managing Australian Government information. To successfully implement an EDRMS, accepted project management principles and techniques need to be followed.

ELECTRONIC DOCUMENT AND RECORDS MANAGEMENT SYSTEMS

What is an EDRMS?

An EDRMS is a software application that manages a range of digital information, including word-processed documents, spreadsheets, emails, images and scanned documents. An EDRMS can combine both document management and records management functionality.

The primary focus of document management is short-term access to, and use of, digital documents created from office desktop applications. For records management, the emphasis shifts to managing information over time for the purposes of evidence, meeting agency business needs, adhering to legislative and governance requirements, and ensuring ongoing authenticity. Some of the functionality that can be combined in an EDRMS includes:

	EDRMS FUNCTIONALITY
Create	<ul style="list-style-type: none"> • Create and collaborate on new documents within the system
Capture	<ul style="list-style-type: none"> • Capture records in a central store for easy search and retrieval • Integrate with common desktop applications (for example, email systems) • Link related records
Describe	<ul style="list-style-type: none"> • Apply approved terms to record titles and names to assist retrieval • Capture and maintain other contextual information (metadata) (for example, creator and date created) • Give records unique identifiers on capture
Secure	<ul style="list-style-type: none"> • Apply security classifications and sensitivity markings • Protect the integrity of information by being able to finalise the authoritative version of the record
Retrieve	<ul style="list-style-type: none"> • Search for information by keyword, record number, creator and other searches • Retrieve stored documents • Restrict retrieval to 'read only' copies when needed
Access and use	<ul style="list-style-type: none"> • Work on or edit documents until they are finalised • Share documents and information to enable collaborative work • Receive and action documents in workflow processes • Apply version control • Apply controls to restrict access
Keep, destroy or transfer	<ul style="list-style-type: none"> • Limit deletion permission • Apply retention periods from records authorities issued by the National Archives of Australia (can be semi-automated) • Capture metadata about deletion

An EDRMS can also be used to automate business processes, such as workflows and approvals.

EDRMS are specifically designed to manage the integrity of, and provide desktop access to, information created using:

- standard office applications, such as word processing, spreadsheets and presentations
- email and other electronic messaging systems
- collaborative work systems
- other applications already installed (for example, imaging systems).

An EDRMS can also integrate and interface with existing paper file systems to:

- register the creation of paper files
- maintain and manage metadata
- improve searchability
- track the movement of physical files
- manage physical storage facilities
- manage the retention, destruction and transfer of paper files over time.

Benefits of implementing an EDRMS

Through improving the management of digital information, an EDRMS can increase business efficiency, provide greater accountability and reduce business risks.

Improved information management capability

- Provide a central store for staff to capture their digital documents and information, instead of in uncontrolled shared drives, email folders or network drives
- Manage email more effectively as records
- Facilitate better retrieval of, and access to, information through greater consistency in naming and titling
- Manage lawful destruction or transfer of records
- Semi-automate records management processes, such as sentencing of records and applying metadata
- Link related documents and records into electronic files or containers
- Allow for integration with other business systems (for example, case management systems) and collaborative work systems to access related information

Increased business efficiency

- Reduce reliance on paper records, and increase savings on physical storage costs over time
- Enable staff to view, read or share information simultaneously from their desktops
- Improve retrieval of, and access to, information by using a central store of digital records
- Reduce duplication by capturing information only once
- Facilitate sharing and reuse of information across work groups
- Potentially streamline and automate work practices and business processes

- Incorporate the ability to search for relevant paper files (if integrated with a paper file system)

Reduced risk to your agency and the Australian Government

- Ensure information is reliable and the latest version is available
- Provide greater security and access control features to reduce the risk of digital information being inappropriately accessed, altered or deleted
- Availability of audit trails to prove who had access to information and what they did with it
- Ability to prove the integrity of information in legal proceedings
- Potential improvement in decision-making through access to the latest, most comprehensive information
- Better ability to service freedom of information applications and discovery orders in a comprehensive and timely fashion

Assist compliance with key whole-of-government requirements

By ensuring records are appropriately managed, secured and accessible over time, an EDRMS can assist an agency to comply with key whole-of-government requirements for the management of information, including:

- *Freedom of Information Act 1982*
- *Archives Act 1983*
- *Australian Information Commissioner Act 2010*
- *Privacy Act 1988*
- *Evidence Act 1995*
- *Electronic Transactions Act 1999*
- *Protective Security Manual* (Attorney-General's Department)
- *Protective Security Policy Framework* (Attorney-General's Department)
- *Australian Government Information Security Manual* (Department of Defence Intelligence and Security)
- *Australian Government Recordkeeping Metadata Standard* (National Archives of Australia)
- *Practice Note CM6 – Electronic Technology in Litigation* (Federal Court of Australia).

Other legislation may also impose specific requirements on your agency regarding the creation, maintenance, accessibility and destruction of particular records.

Use of EDRMS in Australian Government agencies

EDRMS are being used in a range of ways across the Australian Government to manage digital records and information, including:

- moving a paper file system to a digital system
- replacing the use of relatively uncontrolled shared drives, network drives, computer hard drives and personal email folders for the storage of digital information
- supporting workflow systems, such as case management, legal management and project management systems

- providing robust back-end records management functionality to support collaborative work systems.

What an EDRMS cannot do

It is important to be aware of some of the limitations of EDRMS.

An EDRMS alone will not solve all your information management issues

An EDRMS is merely enabling technology. On its own, implementing an EDRMS will not resolve all of your agency's information management issues. Maximising the potential benefits requires improvement in business processes and change in people's behaviour. This includes having business rules, tools and training program in place to guide staff in terms of the capture, naming, access to and use of digital information.

An EDRMS will not provide some types of functionality

EDRMS products and the functionality they provide are continually evolving and maturing. However, the majority of offerings in the current EDRMS market will not provide the following types of functionality:

FUNCTIONALITY NOT PROVIDED	COMMENT
Manage structured data stored within line-of-business systems (for example, Finance, HR and geographical information systems)	EDRMS can be integrated with business systems to: <ul style="list-style-type: none"> • manage outputs such as reports • ensure information is captured only once • enable users to move seamlessly from one system to another to access related information.
Manage the dynamic lifecycle of a web page or system	Enterprise content management systems are generally used to manage the rich functionality of web content and websites. An EDRMS, however, can manage outputs or snapshots of web content. Some EDRMS products have become a key component of enterprise content management suites, while others are moving towards enterprise content management to provide greater functionality.
Advanced document management features	Advanced document management features such as: <ul style="list-style-type: none"> • complex and compound documents (for example, datasets, engineering design files and dynamically linked documents) • document lifecycle management (for example, as required in legal and case practice systems) • drawing and design management are not standard to EDRMS products, and require integration with editing and content management tools. This is possible, but at a premium in price and complexity of design and implementation.

Improving digital information management without an EDRMS

Realising the benefits of implementing an EDRMS takes time, money, resources and effort in improving information management before the rollout.

However, management of digital information can also be improved through other initiatives that promote the systematic and consistent creation and retrieval of records (for example, in email, shared drives and records in business systems).

The National Archives of Australia's records and information self-assessment questionnaire, *Check-up 2.0*, can help to identify areas for improvement. For more information go to the 'Records management' section of the Archives' website at naa.gov.au.

KEY CONSIDERATIONS FOR IMPLEMENTING AN EDRMS

Following are key issues that agencies should take into account to achieve a successful EDRMS implementation.

Resource commitment

Obtain and secure senior management commitment for the required resources.
--

An EDRMS implementation is a major project, requiring a significant commitment of time, money and staff. The resource requirements will depend on factors such as your agency's size, its business needs and the amount of configuration necessary.

Specific tasks that will require resources include:

- understanding your agency's business needs
- documenting your requirements
- selecting an appropriate solution for your agency
- procuring a licence
- engaging with stakeholders and end users, and managing change
- developing your business rules and procedures to operate the system
- configuring the system to your agency's needs
- developing the necessary back-end IT hardware (if it is not already available)
- testing the system prior to implementation
- planning and undertaking the actual implementation
- ongoing training, maintenance and support.

The cost and budget of implementing an EDRMS will depend on:

- the level of functionality rolled out
- the extent of customisation
- the complexity of configuration needed to satisfy business needs
- the work areas of the agency to be included
- the extent of integration or interface with other business systems.

Ongoing resources are also needed to support the operation of the EDRMS once it has been implemented (see 'Ongoing system operation and maintenance' on page 23).

Required skills

An EDRMS implementation is not just an IT project. It involves both rolling out new software, and improving records and information management practices. Close collaboration between records management and IT stakeholders is essential to ensure the broadest understanding of requirements and to maximise the implementation's benefits.

To successfully implement an EDRMS, your agency will need to draw on skills, knowledge and expertise in the following areas:

- records and information management – to set up records management processes
- IT – to work on the technical architecture, systems integration and desktop rollout
- project management
- change management – to manage the impact of change to the way information is created, managed and accessed
- business analysis – to assist business owners to map their business requirements and identify improvements
- information security.

Consider engaging an external consultant with specific experience in EDRMS implementation, particularly if some of these capabilities are not available internally.

Know your agency's requirements

Current and future business requirements

Detailed analysis of current and future business requirements should be done before undertaking an EDRMS implementation project.

This initial analysis will be important throughout the project in terms of:

- determining what the system will be required to do in the medium to long term
- developing a well defined and documented business case
- developing functional specifications and requirements
- selecting the right product for your agency – the overall business need should determine the solution, rather than the technical features of particular products
- determining the degree of customisation or configuration required for the selected product.

For most agencies, a commercial-off-the-shelf application with some configuration will meet most or all business requirements.

Whole-of-government standards and requirements

Key whole-of-government standards and guidelines also need to be taken into account when considering your requirements for an EDRMS.

EDRMS specifications

ISO 16175-1 Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 1: Overview and statement of principles and *ISO 16175-2 Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 2: Guidelines and functional requirements for digital records management systems* should be used by agencies when developing the functional specifications and requirements for their EDRMS. While these specifications provide generic functional requirements suitable for all Australian Government agencies, each agency needs to assess and amend the functional requirements to suit their own business and technical requirements and constraints.

Metadata standards

The *Australian Government Recordkeeping Metadata Standard* describes information about records that the Archives recommends be captured in an EDRMS. It includes mandatory, conditional and optional metadata properties.

ISO 23081 Records Management Processes: metadata for records covers the principles that underpin and govern records management metadata.

Information security standards

The *Protective Security Manual* from the Attorney-General's Department includes principles, minimum standards and procedures for protecting government information from inappropriate access and use. The *Protective Security Manual* can be used only to the end of 2011 as it is being replaced by new policies, protocols and guidelines under the *Protective Security Policy Framework*.

The *Protective Security Policy Framework*, published in June 2010, sets out the Australian Government policy and guidance on protective security. The *Protective Security Policy Framework* supersedes the *Protective Security Manual* and is required to be in place by the end of 2011.

The Department of Defence Intelligence and Security's *Australian Government Information Security Manual* provides minimum standards for ICT security to protect government information when it is processed, stored or communicated by Australian Government systems.

Stakeholder and end user needs

The business needs and technical requirements of the people who will have to use the system are critical and need to be built into the requirements. Doing this from the start will assist you throughout the project, including with:

- the design and configuration of the system – particularly the user interface
- the development of business rules
- identifying the readiness of work areas for an EDRMS implementation
- identifying training requirements
- change management and communication strategies.

Change management

An EDRMS implementation must be viewed as a major change management exercise. An EDRMS does not just involve a shift from paper to digital records. It requires senior management to champion how business information will be managed across the agency. Unless that change is managed effectively, you will not secure the user acceptance and buy-in that is essential for a successful implementation. It is important to have change management and communication strategies in place.

Building trust in the system

An essential change management activity will be building end user trust in the system – this will maximise buy-in and acceptance.

Moving to a new system that people are not familiar with will inevitably generate concerns about how effective and reliable it will be. Common concerns may include:

- What will happen to information if the system goes down?
- Will I be able to easily find what I am looking for?
- Will confidential or sensitive information I put into the system be adequately protected?
- Will using the system make my work more difficult and time consuming?

Concerns such as these will need to be addressed as part of the change management strategy. You may also need to manage concerns about, and negative perceptions from, previous system changes and implementation.

It may be useful to demonstrate the software to individual work groups as this will enable you to identify and address concerns. Also ensure that what is said about the system is backed up by how it actually works when deployed. It is important to test the system in real life situations before the rollout.

Get the information management framework right

Implementing an EDRMS alone will not resolve all your agency's information management issues – this requires getting your agency's information management framework right first.

Understand the current state of information management

An assessment of the current state of your agency's information management, including the systems that are in use and the practices of staff, should be part of your initial analysis. This will assist you with issues such as possible integration with other systems, system configuration and the development of appropriate business rules.

This research is also useful to determine whether or not your agency is ready for an EDRMS. Unless there is a culture of good records management in place, it will be difficult to fully realise the benefits of an EDRMS. It may be that other information management improvements need to be put in place before implementing a new system.

You can use *Check-up 2.0* to assess the current state of your records and information management, and to identify areas of improvement prior to an EDRMS implementation.

Develop or update business rules and procedures to support the EDRMS

Appropriate policies, procedures and business rules will need to be developed or updated to support and guide the ongoing use of an EDRMS. Particular issues that need to be addressed include:

- Will your agency continue to create paper files? If so, will there be particular limitations on this?
- What should be done with incoming and outgoing paper correspondence (for example, will it be scanned and captured into the EDRMS or placed on paper files)?
- If paper correspondence is scanned into the EDRMS, can the paper originals be destroyed? If so, when?
- Which email should be captured as corporate records? Who is responsible for capturing it in the EDRMS, and when?
- How should email attachments be treated?
- How are security and access controls going to be applied in the EDRMS and by whom?
- How will records in the EDRMS be named or titled?
- What should happen when records are created on laptop computers or other mobile devices and social media tools?

Also consider which existing business rules will be superseded once the EDRMS is implemented (for example, 'print to file' rules for email).

Consider how information will be retrieved

One of the most crucial elements of any information system is the ability to search and retrieve information contained in the system. The key to this is to establish some degree of controlled language, for example a set of standard terms or naming conventions that link to your business context. EDRMS applications are designed to upload standard terms and conventions to assist with structuring information.

Naming conventions or other controlled language facilitate better management of information in an EDRMS by:

- linking records relating to the same purpose
- providing greater consistency in titling records by providing standardised headings or keywords that staff must use in their titles
- improving the effectiveness of searching for and retrieving information when required
- facilitating the retention, destruction and transfer of records when linked with records authorities (for example, allocating retention periods when records are created).

In addition to improved business efficiency, business risks will be reduced where a high level of accuracy and speed in locating records is required (for example, in areas of your agency's business subject to frequent freedom of information requests).

Possible options for implementing controlled language include:

- a thesaurus of approved terms – a list of keywords used to identify and locate records labelled with these words. It provides control and consistency over the words (vocabulary) used for titling and indexing records. It does this by providing an alphabetical listing of approved terms that may be used for titling and indexing

- a file plan (sometimes known as a records classification scheme) – a tool for classifying records and other business information, based on the business activities that generate records in your agency.

If your agency has existing naming conventions that are working well and are used by staff, they could be implemented in the EDRMS. If not, they should be developed and tested in consultation with your agency's end users before the new EDRMS goes live.

If you develop a new set of standard terms and naming conventions, consider providing it on the network drives a few months prior to EDRMS implementation. This will allow staff time to become familiar with it first, and any problems with it can be ironed out ahead of time.

See the Archives' *Overview of Classification Tools for Records Management* for more detailed information about naming conventions or controlled language.

Consider how long information needs to be kept

Records authorities are issued by the Archives to authorise the retention, destruction or transfer of agency records. They identify groups of records and provide a minimum retention period for each group. This information can be uploaded into an EDRMS to enable your agency to:

- apply minimum retention periods when records are created ('sentencing on creation') – this can be a semi-automated process
- ensure that records are not retained longer than legally required
- identify which records need to be retained for the longer term, and therefore need to be considered over time in terms of system upgrades.

Implementing records authorities within an EDRMS will enable digital information and records to be managed according to their value over time, so that information is retained for as long as it is required.

All agencies can implement either the Administrative Functions Disposal Authority (AFDA) or AFDA Express. These cover records that relate to the administrative support areas of your agency's business such as personnel, financial management and fleet management.

Your agency may also have one or more existing records authorities covering its core business records that can also be implemented in the EDRMS. If it does not, developing a core business records authority is a major project in its own right. Consider whether it is better to develop one before implementing an EDRMS, or whether it can be left until after implementation.

Also consider extending the application of normal administrative practice (NAP) in your agency to your EDRMS. This will allow for the destruction of low-value records that do not need to be retained under a records authority. For example, NAP may be used for records captured in error or for duplicates in the system.

For further information about records authorities and implementing NAP in your agency, see the 'Keep, destroy or transfer' section of the Archives' website at naa.gov.au.

User permissions

It is likely that staff will have to take greater responsibility for managing their records once an EDRMS is implemented. It is therefore important to consider which records management responsibilities should be delegated from records management staff.

For example, in relation to creating and naming electronic file containers, different delegation options include:

- delegating responsibility to all agency staff to create containers and apply the records classification tool in naming them
- delegating these responsibilities to only a limited number of 'super users' to create and name containers for their colleagues in individual work groups
- retaining central control over creating and naming electronic file containers through your agency's dedicated records management staff.

The extent to which responsibilities such as these are delegated will depend on a number of factors, including:

- state of current records management practices
- complexity of your agency's file plan
- business requirements
- level of risk associated with access to information in the EDRMS
- special security issues.

Integration with other systems

Agencies now use a range of dedicated systems to capture and store business information, including:

- workflow systems such as case management, project management and property management software
- databases
- finance and HR applications
- collaborative workspaces
- websites.

You need to consider the extent to which your agency requires an EDRMS to integrate with these other systems, to what level of integration, and for what purpose. Issues to consider include:

- What are the risks associated with the information and the business it documents?
- What is the value of the records?
- Is records management functionality required to secure the integrity or veracity of the information?
- What are the costs of integration in relation to the likely business benefits?
- Are these existing systems already adequate for their purpose?

EDRMS applications are designed to integrate with common office applications such as email. Commercial 'plug-ins' are also available to integrate EDRMS with other applications such as collaborative software.

With some design and configuration, an EDRMS will also integrate with dedicated business information systems. For example, where an agency has a case management system that captures structured information, an EDRMS can be integrated with it to ensure related unstructured information, such as correspondence, is also captured. Staff can then easily access all relevant information across systems and move seamlessly between them.

In most cases integration with business information systems will require additional specification, design, configuration, testing and implementation, possibly with assistance from an external service provider.

Challenges in undertaking integration can include:

- how to capture and reuse metadata rather than duplicate it
- designing the flow of information between systems
- preserving data integrity in integrated systems
- how to integrate with hard-copy processing tools such as scanning
- compatibility.

Conduct a risk assessment to make decisions about integration with other line of business systems.

Migration from shared drives and legacy systems

In the absence of an EDRMS, your agency will have used a range of different systems to store digital records and information. These could include network drives, work group shared drives and email accounts. Decisions will need to be made early in the project planning stage about the migration of records and information from these existing locations.

The migration of records, data and information from legacy systems can be costly, time consuming and technically challenging. You should approach this issue based on business needs and risks.

Some of the particular issues to be considered include:

- Are the systems to be superseded still 'fit for purpose' and able to provide adequate ongoing storage, access and security for the legacy information and records?
- Do you have content from a system that definitely should be migrated (for example, an existing records management system managing paper records)?
- Will all digital records and information on network shared drives and in personal email accounts be migrated? Will there be a cut-off date?
- How easy will it be to migrate data from other systems?
- Will the data need to be 'cleaned up' (for example, retitled) before migration?
- Is metadata mapping required?

- What level of user involvement do you expect? Will users be expected to clean up their folders and records prior to migration?

Migration approaches should be considered when developing the technical and functional specifications of your EDRMS.

The General Disposal Authority for Source Records provides authorisation for the destruction of records in superseded or legacy systems that have been copied, converted or migrated once certain conditions have been met.

What to do if you are not going to migrate

Your agency will need to properly support and maintain information and records from superseded systems that are not going to be migrated to ensure ongoing access for as long as required for business and legal purposes.

It is also important to have appropriate procedures in place regarding future use of superseded systems. For example, some agencies are disabling their network drives so that all future corporate records must be saved to the EDRMS. However, 'read only' or 'copy only' access is provided to end users so they can access the information they require. You need to choose an approach that allows some flexibility, but also meets the business objectives of the EDRMS implementation.

Future and existing paper records

An EDRMS will reduce your agency's reliance on paper records by enabling records to be managed digitally. For example, email will not need to be printed and placed on paper files. However, an EDRMS may not completely eliminate the need for paper records, and your agency should consider this as part of the planning process.

Future paper records

Your agency will continue handling a certain amount of incoming paper correspondence, such as letters from the public. These can be scanned and captured in the EDRMS, and the paper originals destroyed using the General Disposal Authority for Source Records, provided certain conditions are met. It is important, however, that you develop business rules to guide the process. For example:

- Who will be responsible for scanning and capturing inward correspondence (for example, mail room and registry staff or action officers)?
- Will scanners be located centrally or in business areas?
- What quality controls need to be put in place?
- When and how can the paper originals be destroyed?

There may be legal, security or business reasons to continue keeping certain records in paper format, and these should be identified during the planning process. Common examples may include:

- security classified records that cannot be captured in the EDRMS because of your agency's network rating
- signed copies of contracts, agreements, delegations and other legal documents

- certain personnel records that must be kept in paper format in accordance with the terms of agency certified agreements.

An EDRMS has the functionality to manage the ongoing creation, storage and use of paper records, including:

- file registration
- maintaining and managing file metadata
- recording and controlling the movement of paper files
- managing the retention, destruction and transfer of paper files over time.

Existing (or legacy) paper records

Many agencies are undertaking scanning projects to convert accumulated paper records to digital format to improve accessibility and facilitate greater sharing and reuse of information. Agencies can then reduce their physical storage costs by implementing the General Disposal Authority for Source Records, which authorises the destruction of paper originals if certain conditions are met.

An EDRMS can support efforts to reduce the 'paper mountain' by ensuring the digitised records are properly managed in accordance with key records management requirements.

When making decisions about digitisation of existing paper records, it is important to consider which records should be included and what the anticipated return for investment will be, given that digitisation projects can be time consuming and expensive.

If digitisation of existing paper records is not feasible, a strategy to phase out paper records is required and should include business rules that specify:

- the period of time paper records can be added to existing paper files (for example, until a part is complete or until a specified date)
- certain types of files that need to remain in paper format until a matter is resolved.

Security

Australian Government information security requirements must be implemented as part of an EDRMS project to provide adequate security for the system itself and the information contained within it.

Work with your agency security adviser and IT section to implement the requirements of the *Protective Security Manual*, *Protective Security Policy Framework* and the *Australian Government Information Security Manual*.

Some specific security-related issues that will need to be considered in an EDRMS project include:

- You cannot store records that are more highly classified than your network. You may need to maintain a separate paper file system or more highly classified network to secure highly classified records.

- You will need to develop a security model for your EDRMS to govern how security is applied to control access (for example, the application of security classifications, caveats and other access controls).

Business continuity planning

Loss of digital records in a disaster can be crippling for an agency. Without records, business operations are adversely affected, corporate memory is lost and agencies are vulnerable to greater risk. Agencies should cover all their digital records, information and systems in a business continuity plan.

In planning for an EDRMS implementation, you should identify vital digital records that are essential for ongoing operations and without which your agency could not continue to function effectively. A risk analysis should also be carried out to determine the types of threats faced, the likelihood of disasters occurring, and the potential impact of the resulting loss of records. All reasonable risks potentially affecting your EDRMS should be identified, prioritised and assessed as part of the risk analysis so that steps can be taken to determine appropriate counter-disaster strategies. Work with your IT section on specific counter-disaster strategies, such as regular and comprehensive system backups.

Planning for long-term retention of digital records

There will be digital records in your agency that have retention periods greater than one generation of technology (that is, five to seven years). This poses a challenge in terms of ensuring these records are retained and remain accessible for as long as legal, business and accountability requirements demand.

Key issues that need to be considered in the context of implementing an EDRMS include:

- inevitable hardware and software obsolescence over time
- the need to upgrade systems on a regular basis
- vendors no longer supporting superseded versions of EDRMS software
- processes for identifying and retaining longer-term records, and records that are identified for eventual transfer to the Archives.

Agencies should transfer digital records identified as 'retain as national archives' to the Archives as soon as they are no longer required for business needs.

System configuration

While most agencies select a commercial-off-the-shelf EDRMS, these solutions usually offer a choice of options and will need some configuration to suit your agency's specific business needs.

Particular attention needs to be given to how the system is configured for end users. Issues to consider include:

- Will end users have direct access to the EDRMS or will it sit behind existing systems with which staff are familiar (for example, case management systems or collaborative work systems)?
- What is the best user interface to adopt (for example, a web-based interface)?
- How much functionality will be enabled for end users (for example, will end users have to create and title their own records containers or files in the EDRMS or will this be done by records management staff)?
- What additional metadata does your agency need to collect to better facilitate accurate retrieval and audit (for example, unique project numbers)?

Streamline processes for end users

To maximise system uptake and acceptance, configure your EDRMS to ensure end users find it easy to use without having to understand the underlying architecture.

Ways in which an EDRMS can be configured to streamline business processes for end users include:

- ensuring the EDRMS is integrated with other systems such as email so that records can be captured seamlessly and without having to move between two systems
- auto-populating as many metadata fields as possible to make capture of descriptive information about records less time consuming for end users
- keeping the security model simple – start from the basis that all records are accessible to all users, then add exceptions.

Training

Providing appropriate training is essential to change management and securing end user acceptance and buy-in. A training plan should be developed early in the project. This will assist the project team to understand the training needs for all levels of staff, tailor training to target specific needs of individual business areas, and identify resources required to implement the training plan.

Records management training

Staff may need to take more personal responsibility for managing records once an EDRMS is implemented – they will need to know basic things such as what to keep, how to name it, and when security and access controls should be applied.

In preparing staff for an EDRMS, it can be extremely valuable to start by providing general records management training. This will help improve records management practices before the system is implemented.

Agencies can use or adapt the Archives' *Keep the Knowledge: make a record* package to provide this type of training.

Staff will also need specific training in any new business rules or tools that have been put in place as part of an EDRMS implementation, such as how to use a new file plan or records classification scheme.

EDRMS training

Staff will need training in how to use the new EDRMS. Some suggestions to consider when developing this technical training include:

- Different training modules should be developed to cater for the needs of different user groups (for example, general users, users with higher levels of records management responsibilities and system managers).
- Different approaches to training (for example, group sessions or one-on-one sessions) can be effective in different situations and circumstances.
- Ensure that the EDRMS (with all required functionality) is available to staff as soon as training has been completed. System implementation risks increase if there are long delays between staff being trained and being able to use the system.
- There should be resources to support users as soon as training is completed (for example, cheat sheets, 'floor walkers' and a help desk service).

Ongoing training and support

Agencies should also ensure that training does not stop when the implementation does. There will be an ongoing need to train new staff, and refresher training should be available to existing staff.

Pilot before rollout

Given the impact an EDRMS will have on your agency and staff, it is absolutely essential that agencies get the implementation right the first time. For this reason, it is advisable to conduct one or more pilots before rolling out the system. Doing so will enable you to:

- test functionality on individual platforms and in real life situations
- iron out any technical bugs that emerge and make necessary changes
- test the readiness of your agency for an EDRMS, and identify areas needing improvement (for example, general records management awareness)
- decide on the most appropriate rollout option (see below).

Targeting particular business or work groups to participate in a pilot can also be a valuable way of obtaining 'champions' for an EDRMS, and in promoting the benefits throughout the agency.

Choosing the right rollout option

There are three main options for rolling out an EDRMS:

- a 'big bang' approach, where the EDRMS is rolled out to everyone across the agency in one go
- a phased approach, where the EDRMS is rolled out to different work areas or groups of staff over time
- a combined approach, where limited functionality (for example, integration with desktop applications) is delivered to all users at the same time. Additional functionality (such as integration with email and other business systems) is then progressively added.

Factors that can help you determine which rollout option is most appropriate for your agency include:

Agency size and structure	A phased approach may be more appropriate if your agency has a large number of staff and/or staff located across dispersed locations.
Degree of customisation required	A phased approach means that the EDRMS can be tailored specifically to address work area needs, requirements and business processes.
Uniformity of business practices across agency	If business practices are more or less uniform across your agency, a 'big bang' approach may be appropriate.
Current state of records management	If records management needs improvement, it may be best to adopt a phased approach.
Risk assessment	If implementing an EDRMS is assessed as high risk, it may be best to adopt a phased approach, which can minimise the impact of realised risks.
Quality of data to be migrated	A 'big bang' approach may be considered an acceptable approach if only minimal data clean up is required.
Ongoing use of old systems	If ongoing use of old systems is required for a period of time, then a phased approach may be more appropriate.
Degree of change management required	If staff need to learn more than just how to use the system, a phased approach may be better.
Will immediate access to the EDRMS be required across the agency?	The 'big bang' approach will be more suitable if this is the case.

Ongoing system operation and maintenance

EDRMS implementation will not be an 'install once and walk away' experience. Your agency will need to make an ongoing resource commitment to support the operation and maintenance of the EDRMS, including:

- system administration
- quality assurance
- software upgrades
- reconfiguration and enhancement (over time)
- user training and support (for example, help desk service).

It is important to make sure that corporate responsibility for these ongoing activities is defined well before the implementation project comes to an end.

REFERENCES

- Attorney-General's Department, *Protective Security Policy Framework*, Attorney-General's Department, Canberra, 2010, http://www.ag.gov.au/www/agd/agd.nsf/Page/ProtectiveSecurityPolicyFramework_ProtectiveSecurityPolicyFrameworkDownloads.
- Attorney-General's Department, *Protective Security Manual*, Attorney-General's Department, Canberra, 2006, [http://www.ema.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_ProtectiveSecurityManual\(PSM2005\)](http://www.ema.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_ProtectiveSecurityManual(PSM2005)).
- Department of Defence Intelligence and Security, *Australian Government Information Security Manual*, Department of Defence Intelligence and Security, Canberra, 2009, <http://www.dsd.gov.au/infosec/ism.htm>.
- Federal Court of Australia, *Practice Note CM6 – Electronic Technology in Litigation*, Federal Court of Australia, 2009, http://www.fedcourt.gov.au/how/practice_notes_cm6.html.
- International Organization for Standardization, *ISO 23081 Records Management Processes: metadata for records*, International Organization for Standardization, Geneva, 2006.
- International Organization for Standardization, *ISO 16175-1 Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 1: Overview and statement of principles*, International Organization for Standardization, Geneva, 2010.
- International Organization for Standardization, *ISO 16175-2 Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 2: Guidelines and functional requirements for digital records management systems*, International Organization for Standardization, Geneva, 2011.
- National Archives of Australia, 'Keep, destroy or transfer', National Archives of Australia, Canberra, September 2010, <http://www.naa.gov.au/records-management/keep-destroy-transfer/index.aspx>.
- National Archives of Australia, *Check-up 2.0*, National Archives of Australia, Canberra, 2010, <http://www.naa.gov.au/records-management/check-up/index.aspx>.
- National Archives of Australia, *Australian Government Recordkeeping Metadata Standard Version 2.0*, National Archives of Australia, Canberra, 2008, <http://www.naa.gov.au/records-management/create-capture-describe/describe/rkms/index.aspx>.
- National Archives of Australia, *Keep the Knowledge: make a record*, National Archives of Australia, Canberra, 2007, <http://www.naa.gov.au/records-management/training/Keep-the-Knowledge/index.aspx>.

National Archives of Australia, *General Disposal Authority for Source Records that have been Copied, Converted or Migrated*, National Archives of Australia, Canberra, 2003
<http://www.naa.gov.au/records-management/keep-destroy-transfer/authorities/gdas/gda-source.aspx>.

National Archives of Australia, *Overview of Classification Tools for Records Management*, National Archives of Australia, Canberra, 2003,
http://www.naa.gov.au/images/classification%20tools_tcm2-1030.pdf.