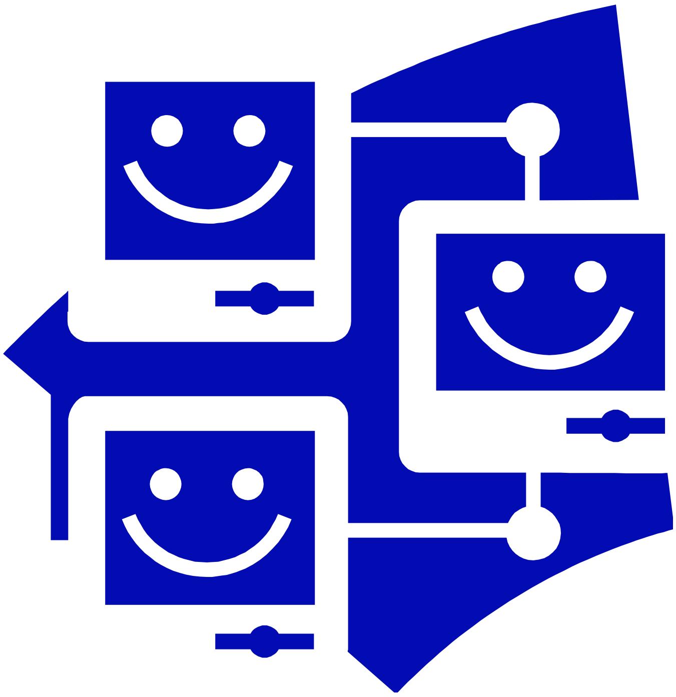
Evidence Element 7 – appendix 20

Managing a Digital Information Migration Project

to ensure future preservation of electronic information across electronic document and records management systems [EDRMS]



Eleanor Rowe

Records & Information Management

Name of document	Managing a Digital Information Migration Project to ensure the future preservation of electronic information across electronic document and records management systems [EDRMS]
Author:	Eleanor Rowe, Records Manager
Description of Content:	Guidance for preservation or migration of information between electronic systems – future proofing for electronic information to ensure business continuity. Exit strategy for obsolete systems ensuring information is safeguarded.
Consultees	Paul Hassan Roy Poulsen Jeanette Netherwood Mike Alexander David Morris
Distribution:	All staff
Embargoed	No
Status:	Draft
Approved by:	
Date of Approval:	

1 Introduction

Digital continuity is the ability to use information as required for as long as it is needed.

Digital continuity is put at risk by change – including changes to how information is used and managed; the organisational structures that govern it and the technology used to create, store and access it. Information must be managed carefully over time and through changes to maintain the usability and authenticity needed.

1.1 Scope

This guidance will help prepare for migrating information between Electronic Document and Record Management Systems (EDRMS) and focuses on maintaining the continuity of the information.

This guidance will help staff to understand:

- why migrating information between EDRMS poses risks to digital continuity (the ability to read electronic documents in the future)
- how to define information and migration requirements
- the key risks to digital continuity to watch out for in undertaking a migration.

This guidance does not:

- provide advice on choosing or configuring a new EDRMS, nor does it cover all the technical aspects of moving to or implementing a new EDRMS
- provide detail on every aspect of managing an EDRMS migration project, only those elements and risks that affect the usability of the information.

Some elements therefore, such as education and training, changing business process and communications are not covered here, but will need to be managed as part of the overall migration or EDRMS implementation project to ensure its success.

There are several reasons why information has to be migrated from one system to another - for example, changes in business practice, changes in technology, the end of a contract on one type of system or implementing a different EDRMS.

This guidance is applicable to all information held within an EDRMS and does not make a distinction between ‘documents’ and ‘records’ or between various different document/content types and formats. Although aimed primarily at EDRMS migrations, many of the planning principles and risks could apply to other data migration projects.

1.2 Audience

This guidance is aimed at the member of staff leading or managing a project to migrate information between EDRMS.

The guidance will also be useful for those managing or implementing the technical aspects of the migration to provide them with a better understanding of the key risks to the continuity of the information.

1.3 What is digital continuity?

Digital continuity is the ability to use your information in the way you need, for as long as you need. If you do not actively work to ensure digital continuity, your information can easily become unusable. Maintaining your digital continuity requires active management of your information through change so that it remains complete, available and therefore usable in the way that you need. In practical terms, your information is usable if you can **find, open**, **work with** it, **understand** it and **trust** it.

2 Risks involved in EDRMS migration

EDRM Systems provide complex mechanisms and structures for organising and providing access to information. Different systems and versions will handle, display and organise the information they hold very differently.

Moving information from one form of data structure and technology application to another raises the risk of loss of some or all of the information content or context, or your ability to access it, so that users:

- can’t **find** the information needed
- can’t **open** the information needed
- can’t **work with** your information in the way needed
- can’t **understand** what the information is, or what it is about
- can’t **trust** your information is what it says it is.

EDRMS migration requires careful planning and management to ensure that staff:

- understand how to use the information
- maintain the completeness, availability and usability of the information throughout the migration process
- manage the risks involved in migrating information between systems.

ensure that the EDRMS into which the information is being migrated has the properties needed to ensure digital continuity – such as capability to import and export information effectively, facilitating further changes in the future.

3 Preparing for successful information migration between EDRMS

Information held in the EDRMS is likely to be critical to your organisation’s business operations. This means that any activity that puts the use of this information at risk needs to be managed appropriately.

Transfer of content between systems can be a highly demanding process, involving a number of distinct stages, each with an associated risk and cost. An EDRMS migration must be planned and managed as a significant data migration, business change and technology project. A range of skills, resources and processes will be required, in addition to the technical capability to carry out the physical transfer of content.

Risks increase when EDRMS migrations are not managed as well-structured projects, when they do not involve personnel with the relevant skills and expertise, or include representation from across ICT, information management, information assurance and business management.

For example there's a risk if the migration is an ICT led technical exercise that does not sufficiently engage with the business requirements for information. Conversely, there will be increased risks and issues if ICT teams are not engaged early to inform the business and information management teams of the technical constraints and opportunities that will influence how the migration can be implemented.

Finally, undertaking an EDRMS migration can incur significant costs, both in terms of resources and expenditure for specialist expertise and supplier action.

3.1 Key principles for managing your EDRMS migration

EDMS migration is more likely to succeed using these six key principles:

1. **Manage it as a project**: establish a strong project structure and management process to deliver the EDRMS migration. Include expert project management support and project governance that is tied in to the business and owned at the appropriate level. Project management will help you to manage risk, and to deliver the migration process successfully and help you to ensure the migration is within time, quality and budget constraints.

2. **Take time to plan**: taking sufficient time to plan up front, gathering information requirements and understanding the risks involved in moving information between systems, is absolutely critical to ensuring success. A suitable planning stage will help manage the migration more quickly and easily and improve risk mitigation.

3. **Involve the right expertise:** ensure the right people are involved with the right skills, including people who understand the business requirement, ie stakeholders, and those who understand the technology and information structures. A cross-disciplinary project team involving staff from information management, ICT and information assurance functions, business continuity would be ideal.

4. **Lead with business requirements**: understand the outcomes to be achieved, namely how the business needs to use the information which is being migrated. Ensure ownership of the requirements at the appropriate levels – for instance, Information Asset Owners (IAOs), Senior Information Risk Owners (SIROs) or heads of the business units that depend on the information. This will help decide what, when and how to migrate ensuring identified outcomes are achieved and maintaining digital continuity in the process.

5. **Manage risks carefully**: EDRMS migration poses a risk to digital continuity, so a risk management assessment must have been done in advance. Make identifying and controlling risk a key part of how the project is managed, including ownership of the risks (including the business risk of information not being fully usable following migration) at an appropriate level – most likely you will involve someone at executive level, such as a SIRO. This will help to

identify risks inadvance and avoid or mitigate them before issues arise.

6. **Test for continuity**: frequent and extensive testing prior to and following the migration will help ensure issues are identified and addressed before they arise. Once this is done to a satisfactory standard for all concerned the old EDRMs can be disposed of and staff can move confidently to using the new EDRMS.

4 Managing the migration project

4.1 Roles and expertise to involve

Capability	Why it matters
Project management	Overall management of the process, reporting, delivery against the required outcomes.
Stakeholders – services	How the business needs to use its information. Will draw on expertise within services and needs to understand the legislative environment, involving specialists in Data Protection, Freedom Of Information, Record Management, Information Assurance etc
Risk and issue management	Identifying and managing risks and issues at each stage of the process. Impact assessment of migration decisions on the continuity of the information and delivery against the required outcomes.
Contract/supplier management	Liaison with IT suppliers (service providers, software vendors, implementation partners, specialist ICT services). Understanding service levels and managing costs.
Testing	Testing of processes. Testing whether migrated information continues to meet requirements (testing for continuity).
Information architecture and/or data migration expertise	Developing the migration process. EDRMS administration, information architecture, design and interpretation, data transformation, export/import mechanisms, secure transfer, decommissioning and disposal.
Information assurance, security and access control	Identify and manage any IA risks and security processes. Establish required access control.
Information governance (FOI, DPA)	Inform requirements and testing to ensure compliance with relevant policies and legislation.

4.2 Managing single or multiple third-party suppliers

Local Government ICT is often provided and managed by specialist external service providers, under contract to the department. To ensure digital continuity during transfer liaise with service provider to clarify responsibilities for the work, agree the support they will provide, and understand any associated costs.

Procurement or supplier/contract management function may be able to assist with this. The key contact or account manager for the supplier should also be able to offer advice.

If EDRMS migration is being managed by suppliers, then the following steps to help manage the risks associated with this type of project:

- **Define very clear requirements**, framed as business outcomes that the migration has to enable, and ensure these are agreed with and communicated to the suppliers prior to the migration.

- **Establish clear, detailed acceptance criteria** that will test whether your business outcomes have been met, with appropriate performance measures for maintaining data quality, usability, and performance. Agree this with the supplier prior to the migration, and agree and document any exceptions where the supplier states that it is unlikely or impossible for them to meet the criteria. Clear requirements and acceptance criteria are particularly important if the supplier will not provide technical detail on their migration process, or there is no in-house expertise to assure their plans.

- **Ask suppliers to detail how they are going to meet requirements** prior to the migration, to enable the project management team/ICT to assure their process and confirm it is likely to meet needs. Request detail on the schema mapping and procedures for migration.

- **Ensure that suppliers contribute to risk and issue management**, and share their assessments of the risks and issues associated with the migration, and their plans for managing these.

- **Ensure that where multiple suppliers** are involved in a migration that the project team facilitate communication and co-ordination between them and regularly check that this communication is ongoing – for example, where one supplier is handling the export, another the import, and potentially another providing core IT services. Request that suppliers provide documentation on how they plan to manage this co-ordination and liaise with the other supplier(s). If multiple suppliers are involved, establish who is responsible for delivering which component of the migration and who is responsible for managing which risks. Clarify who is the lead supplier for the migration project, and hence responsible for managing the co-ordination with other suppliers, and ensure they explicitly accept this role.

- **Request proof-of-concept and testing from your suppliers** to demonstrate the likely success of the migration prior to it being executed in a live environment.

- **Ensure that suppliers provide details on how they will address the security** of the content throughout the process, particularly if the EDRMS contains personal and sensitive data.

5 Defining business requirements

Defining business requirements for the information which is being migrated between EDRMS systems is the critical first step. Do this before planning or undertaking a migration.

Need to identify the following:

- what information the originating EDRMS holds – and what may need migrating
- how the business needs to use the information
- whether migration is the right response
- what information is to be migrated
- how to maintain the digital continuity needed through the migration

5.1 Define what information is affected and how it is used

Before starting EDRMS migration a high-level understanding of what information assets will be affected by the change, how the business needs to use this information, and the key outcomes to be achieved must be gained. This will help inform whether migration is the right approach, and shape the migration process itself.

The overall aim of an EDRMS migration is to enable business and operational continuity by ensuring that the information remains available and usable by the business. Understanding this business need for the information is therefore the crucial first step towards building overall requirements that will drive and govern the migration process.

At this stage, there is no need to identify very detailed requirements- just need to understand enough about the information to decide whether migrating the information between EDRMS systems is the right approach.

Questions to ask include:

- Do staff still need regular access to the information?
- If so, who needs access and how quickly?
- Are you migrating all the information, or part of it? Can you clearly identify what part?
- How do you need to use the information? For example:

Is it needed for daily operational processes?

How do staff need to read, edit, re-use, print, publish, share or otherwise make use of the information?

Is it being kept for reference, audit or accountability purposes only?

Is it required to enable the business to meet its statutory obligations? (e.g.

Freedom of Information, Data Protection and Environmental Information

Regulations)

Is it being kept for historical preservation, to form part of the public record – the Council Archives?

- Can you dispose of some or part of the information?

- Is the information still within its retention period? If no retention period has been set, do you still need to keep the information? How long for?

Your organisation may have an Information Asset Register (IAR) or similar list where your usability requirements for your information have already been gathered. Liaise with your information management team and relevant IAOs to make sure this information is correct and up to date

5.2 Decide whether EDRMS migration is the right approach

A high-level understanding of the information means being able to confirm if migrating the information between EDRMS is the right approach to take.

EDRMS migration is a costly, risky and complex exercise and should not be undertaken until it is certain that there is a business need.

The migration as an opportunity to review the information in use, evaluate what to keep, and reduce overall data volumes by disposing of information.

Alternatives to EDRMS migration include:

5.2.1 Leaving the information where it is:

In the original EDRMS, if it remains available: This may be appropriate where information has a short retention period and is no longer in active use. In such cases, the cost of migration may exceed the cost (and risk) of supporting the information within the original system, until it is disposed of in line with its retention schedule. The downside of this approach is that, for a short period, information may be less easy for users to find.

5.2.2 Archiving the information:

Into an archive system: If information isn't in regular and active use, but it is of continuing business value or of enduring historical interest migrate it from the EDRMS to a more suitable platform. 'Archive' environments generally offer some of the features of an EDRMS (hold structured content associated with descriptive information) though often with reduced functionality, lower performance, and lower cost.

5.2.3 Disposing of information

If information is no longer required by your business, disposing of it is a preferable alternative to migration.

5.3 Identify what to migrate and what to destroy/dispose of

If EDRMS migration is the right approach to meet business needs decide whether to migrate all the content of the EDRMS, or just some of it. If it is only a partial transfer this needs to be clearly identified based on what information continues to be needed. There must also be a strategy for disposing of the information which is not being migrated.

5.4 Define detailed digital continuity requirements

The final critical stage is to turn the detailed knowledge about what is to be migrated into more detailed digital continuity requirements for the information to be migrated. This means identifying how the information to be migrated will be **complete**, **available** and therefore **usable** following the migration.

Focus on the information which must be retained rather than the functionality of the technology, i.e. from a users point of view rather than an ICT viewpoint. How you the information is created, used and stored will inform the specification and configuration of the receiving EDRMS, and the functionality needed from the new system

Identify what is required for the information to be:-

- **found** (located effectively by the user)

- **opened** (viewed in available technology applications)

- **worked with** (as needed, such as read, edited, printed, published, re-used)

- **understood** (interpreted correctly by the user)

trusted (relied upon by the user as suitably authentic, accurate or timely, including suitability to be used as evidence if required).

Refer to the Information Asset Register (IAR) or similar list. Liaise with the information management team and relevant Information Asset Owners (IAOs) to make sure this information is correct and up to date and agree any changes to usability requirements that have been identified as part of this migration process.

Depending on the type of information held in the EDRMS will inform the best level of detail at which to define requirements. For example:

- define a generic set of requirements for all information to be migrated

- define a varying set of requirements for the information which supports a particular business need

- define a specific set of requirements for all information of a particular type or file format.

What completeness and availability means, at a high level, is covered below. For more detail on the specific questions needed to produce detailed requirements, see the Appendix 1.

5.4.1 Completeness

What content, context and provenance information do are required to allow the information to be used as required?

- Content

Content is the core information found within the EDRMS. Once the different document/content types and formats to be migrated have been identified – further detail is required e.g. what metadata, version histories, renditions and embedded objects and attachments will be required for the information to be complete and fully usable?

- Context

The context of information is the associated record of the circumstances of its creation and use. It's what enables staff to find, work with, understand and trust information. Context can be provided through a number of different sources. It will be necessary to identify what contextual components to migrate alongside the content and how the crucial link between the two will be maintained. Context can be provided by links between documents, shortcuts and references, location in the classification scheme or file plan, contextual and management metadata for the document, such as dates, authors and retention schedules.

- Provenance

The provenance of the information is the associated understanding of its origins, custody and ownership, which enables the user to understand its source and authenticity. This is often provided through metadata automatically generated by the EDRMS.

In addition, the system may record a range of information that supports the evidential weight of information, which needs to be kept if this is a business need. See *BS 10008:2008 – Evidential weight and legal admissibility of electronic information* for further details.

Need to decide whether there is a need to migrate or retain access to provenance information, such as audit trails and logging, source and rights metadata or digital signatures.

5.4.2 Availability

Sldo need to decide what will be required to be able to find, open and work with information to support business needs?

Consider how users will search for or identify the location of the information; the access controls that need to be in place; and how to manage encrypted or password protected information. Identify what file formats the information to be migrated is held in.

5.5 How to use your digital continuity requirements

Once the digital continuity requirements are known it will be easier to manage to manage and plan moving the information from one system to another - the key components of the information held in the EDRMS will have been idenified which alongside the content, will need to be in place in the new system to enable the usability required.

These requirements will allow the project management team to do the following:

5.5.1 Communicate usability requirements to the wider project team

This can help to ensure that everyone working on the project has a shared understanding of what is to be achieved through the migration.

5.5.2 Specify the functionality required from the new EDRMS

Understanding what must be transferred from the old to the new will help pecify sdetailed import and export functionality for a new EDRMS. For example, when thinking about metadata, the new EDRMS must have the functionality to hold, record, report and search against certain metadata and the metadata from the old EDRMS must be maintained and transferred.

5.5.3 Manage changes to requirements

If there are technical, financial or business constraints on the EDRMS migration project a compromise on how the requirements are met. A detailed picture of the requirements will inform negotiation with suppliers, technical staff and the business, with clear understanding of the business impact and risks associated with any changes to the requirements.

5.5.4 Shape the migration implementation and testing

The requirements should inform the acceptance criteria for migration between systems and be used to agree requirements and acceptance processes with any external parties managing the process.

In selecting a new EDRMS, ensure that the system you being procured and migrated to has good continuity properties (for example, good import and export facilities). This will enable migration issues and risks to the continuity of your information in future to be minimised.

Remember to consider:-

- export-import checklist
- export-import routes
- verifying the data transition
- XML schemas for migrating EDRM information

6 Managing key risks and issues

EDRMS migration carries many risks and the success of the project can depend on careful risk management. It is important that the impact on the business of not being able to use the information in the way required during and following the migration – and ensure that the business is aware of these risks.

Consider risks such as:

- poor project or supplier management
- technical constraints, impacting system performance or users, from the migration process itself
- technical or business process constraints on the ability of the migration to deliver business requirements.

There are some key risks to digital continuity to look out for. Many of these relate to comparing how the two EDRM systems handle and interpret the information and its use and access, so that the digital continuity needs continue to be met, even if the functionality of the two systems differs. But there are also risks to manage around information governance, ownership and business process, which can all contribute to the migration not meeting requirements. The rest of this section focuses on the **key risks to digital continuity which include**:

- understanding requirements in sufficient detail
- constraints in the technical capability of the originating and receiving EDRMS
- updating information governance and business processes.

6.1 Understanding requirements

Not understanding information requirements thoroughlymay result in not realising that the migration does not provide what is required until it is too late.

EDRMS are all different and rarely present and handle information in the same way, so compromises in requirements may be needed. Identify what requirements are business critical, and which are only desirable, to help prioritise. May also choose to reduce the scope of the requirements.

6.2 Constraints in the technical capability of the EDRMS

EDRMS often behave differently, are not directly compatible and have not been designed for easy import and export of information. This can impact on the ability to meet requirements.

If there are constraints over what the new EDRMS can do there will be an increased number of issues and risks.

To plan the migration and assess risks effectively need to understand:

- how one system exports and the other imports
- how the two systems handle metadata
- how the two systems handle the files/objects (containing the content)
- how the relationships between the two are managed within each system
- whether there are information types or formats that cannot be handled by the importing system.

This will inform the technical work needed to ensure that the metadata, content and associations can be transferred between the two systems. Key risk areas to explore include:

6.2.1 Export and import capability

If the EDRMS doesn’t have an export facility, this will increase the risks around migrating information, as it is more likely that key information could be lost, particularly metadata, or links between information. Objects (files with the content) can become disassociated from their metadata or related information objects if import/export functions do not maintain links, or if there are data quality issues affecting the association.

Even when an export function is available, it is rare that an EDRMS export captures everything held in the system.

Similarly, the import functionality on the receiving EDRMS may not be able to handle all the information to be migrated.

Questions to identify risk:

- Does the EDRMS export information? Does it do so in a form the receiving EDRMS can import?
- Can the receiving EDRMS import information?
- Does the import/export cover all the required information - content and all associated metadata? How is the metadata associated with the objects (content files)?
- Can the receiving EDRMS maintain these associations in the same way or will new associations be needed?

6.2.2 Data integrity

There is a risk that the receiving EDRMS will not be able to accommodate or display the metadata in a way that is comparable to the originating EDRMS. This could make the information more difficult to find, understand or trust. There is a risk that this could be misleading, for example if data appears in a field with a different description, or is not available to the user.

There is also the risk that critical metadata fields will be changed on migration. Dates are particularly vulnerable to change when files are migrated. For example, the date of creation may be reset to the date of migration. Pay particular attention to dates in the test plan. For more information on the risks associated with metadata see the Appendix 1.

Questions to identify risk:

- Can the required information be accommodated within the receiving EDRMS? Does the receiving EDRMS display the data in the same way?
- Are there metadata fields that will not be viewable by the user, or not displayed with the same description?
- Does the receiving EDRMS amend date – or any other – fields on import?

6.2.3 Data quality

Not every system will handle data in the same way, and the quality of the data may impact on the success of migration. Different systems have varying tolerances for data quality or structure. Data quality issues in the information being migrated may affect the ability of the receiving EDRMS to display or process the information correctly.

For example, one system may accept partial dates (MM/YY only) whereas another requires full dates (DD/MM/YY). Migrating date information between these two systems will cause issues or inaccuracies in the data, such as blank fields (losing the partial date information) or inaccurate data (defaulting to 01/MM/YY when incomplete, for example).

Data quality improvements and amendments typically need to be undertaken prior to migration to reduce cost and risk.

Questions to identify risk:

- Does information held in the originating EDRMS have data quality issues?
- Will poor data quality impact upon how the information is found, used and displayed in the receiving EDRMS?
- Do you need to consider changing the data to improve quality before migration?

Further detail on technical capability risks to your requirements can be found in the Appendix 1.

6.3 Updating information governance and business process

6.3.1 Information governance and ownership

As the migration carries significant risk need to ensure that the appropriate information governance structures and accountable staff such as Information Asset Owners (IAOs) are in place. Provide visibility of the project and risks at the right level, including up to the Senior Information Risk Owner (SIRO) [Head of HR & ICT] if the EDRMS contains business critical, personal or sensitive information.

Clear ownership for the information, before and after migration, must be established. It is particularly important to ensure information is transferred appropriately if the EDRMS migration is due to changes in the organisation structure. Update IARs, policies and procedures to reflect the new location of the information. Allocate new IAOs, if required, to ensure that the information ownership is transferred effectively alongside the technical migration of the data.

6.3.2 Business processes

There will be a need to identify whether to make any changes to the business process for managing information subject to migration, to meet requirements. By introducing a different EDRMS, and potentially moving information into a different system, it is likely that different business processes may be adopted. If this is not considered, there is a risk that information will still not be usable, even if the technical capability is there. It might be that a new process or procedure is mitigation of a technical risk or issue, if the receiving EDRMS cannot meet a requirement.

These new business processes might affect users of the information, who need to understand a new way of finding, opening and using the information they need. It is most likely to impact on those responsible for managing the information, who will need to get to grips with new technology and capability, alongside new policies and procedures.

Remember to include the need for training and communications to transition to the new business processes alongside the new technology.

7 Testing for continuity and completing the migration

The final stage of the EDRMS migration project is to test for the continuity of the information.

Refer back to the requirements and acceptance criteria first defined and develop acceptance testing processes that fully test whether each requirement has been met.

Always always aim to perform multiple test and pilot migrations before undertaking the final migration to ensure that success is likely and any issues ironed out in advance. However, it is vital to test fully after the full migration. It is also vital that tried and tested 'roll-back' plans and procedures are in place, so that in the event of the migration failing or new issues arising, it is possible to revert to the pre-migration environment.

Always aim to involve the users of the information in the acceptance testing process.

Once confident that the migration has been a success, the information held in the originating EDRMS can be disposed of and that system can be decommissioned.

If there is information that it was not possible to migrate successfully retain the originating EDRMS for a period to migrate or otherwise manage access to this information – though this is expensive and should only be considered for clear business reasons and for a defined, limited period.

Finally, be sure to update IARs, policies and procedures to reflect the new location of the information, allocating new IAOs if appropriate, to ensure that the information ownership is transferred effectively alongside the technical migration of the data.

8. Further information

Further information about digital continuity can be found on the National Archives website

Appendix 1 – Requirements and Risks

This section provides further detail on the key areas to be considered when defining the requirements from EDRMS migration, and indicates additional potential risks to watch out for in meeting those requirements.

Completeness of the information

Ensuring that the information remains complete following migration involves considering the content, context and provenance needed in order to use the information. This includes:

- Metadata
- Classification scheme and filing structure
- Versions and renditions
- Embedded objects and attachments
- Links between documents shortcuts and references
- Audit trails and logging

Metadata

Metadata elements may describe the content of an information asset, such as title, subject, description, keywords. This can be automatically generated by the EDRMS, or user-defined.

Contextual metadata: The EDRMS will also hold a large number of metadata fields that do not form a direct part of the information content, but provide additional context on when and by whom the information was created, modified, used.

Management metadata: The EDRMS will hold metadata related to the management of the information that do not form a direct part of the content but provide additional context on how the information is handled and a guide to how the information should be managed.

Source and rights metadata: Source and rights metadata can indicate the source and ownership of the information, and may describe previous transfers between organisations, indicating its provenance.

Questions to identify requirements:

- What existing metadata will be needed in order to find, use, understand and trust the information? e.g. metadata about:
    - roles (author, owner, editor, contributors, etc)
    - dates (dates created, revised, published)
    - source and rights (owner, source organisation etc).

- What existing metadata is needed to manage or handle the information appropriately? e.g. metadata about:

  - retention schedules (review or disposal dates)
  - protective marking
  - sensitivity review.

- Do you need all the existing metadata or just a key sub-set?
- What would be the impact if the new system did not have this metadata?
- Is the metadata complete in the originating EDRMS or are there data quality issues (metadata missing or incorrect)?
- Have you identified where you need user-defined metadata, rather than just what the EDRMS records automatically?

Metadata risks

There is a risk that the two systems will have very different metadata schemas and interpret the data in different ways.

Alongside mapping data fields, it is important to understand how the receiving EDRMS uses and displays that data, to see whether it does so comparably with the originating system. Data fields that *appear* comparable based on description eg ‘date’, ‘author’ may be used differently, and change the apparent meaning of the information for the user. Need to understand how the receiving EDRMS interprets and displays its metadata before deciding how to map the existing metadata across.

There is a risk that information flagged as sensitive will not be marked as such in the receiving EDRMS if this metadata cannot be mapped or migrated. If sensitivity markings interact with access controls and permissions, this will add an additional level of complexity that will need careful management to ensure that sensitive information is not inappropriately handled or accessed.

There is no industry standard output for EDRMS so some bespoke development is likely to be required to map the two data schemas together. Extensive testing must be done to ensure you maintain the completeness of the information when migrating metadata.

Questions to identify risk:

- Can the critical metadata fields be exported/imported?
- Do the metadata schemas of the two EDRM Systems align?
- Are there places in the receiving EDRMS metadata schema that can map all the metadata needed?
- Do the fields in the receiving EDRMS handle and use the metadata in the same way?
- Does the metadata indicate whether information is personal, sensitive or protectively marked?
- Does this metadata govern how the information is accessed and handled?
- Will this metadata and functionality be replicated on the receiving EDRMS?

Classification scheme and filing structure

Context is often provided by the position of the information in the file plan or filing structure. This can help the user understand what business purpose the information serves, or how and why it (and any associated information) was created and used. Information can become unusable without this additional context. A lower-level folder entitled simply with a date, for instance, tells the user very little about its contents.

To maintain the context of the information in the form of its location in the original file plan or organisation structure, it is important to ensure that this contextual folder structure can be migrated alongside the content and metadata.

Questions to identify requirements:

- Can staff find and understand the information without the context provided by its position in the filing structure?
- Do the titles of high-level folders form part of the description of the information?
- Will you need to replicate the classification scheme or filing structure in the target EDRMS?

Filing structure risks

If contextual location information cannot be located, there is a risk that there will be a need to manually recreate the file plan and move information into the right place. If the original structure cannot be replicated this information may need to be held in an additional metadata field or to include it with the new file or document title to provide the context required.

Conversely to integrate the information into the receiving EDRMS file plan, map each area of the source classification scheme to its equivalent in the destination classification scheme – which may need to be amended to accommodate it. Trying to move records from a functional file plan into an organisational file plan (or vice-versa) can be difficult and can lead to inconsistencies in where files are put.

Questions to identify risk:

- Can the contextual information encoded in the folder structure/file plan structure be migrated?
- Does the import/export function maintain location within the file plan?
- Is the destination file plan organised on the same principles as the source file plan?

Versions and renditions

Content managed within an EDRMS may include multiple different versions of the same document. For example: versions produced as a mechanism for tracking changes to the document; or redacted versions produced for publication.

A rendition is an instance of a record rendered into another software format, (eg creating a PDF of all documents). The content and most metadata will be identical. Renditions may be required for preservation or access/viewing purposes.

Questions to identify requirements:

- Does the originating EDRMS hold different versions of documents?
- Need to refer back to these versions or need to keep them for audit purposes?
- Need to access and use renditions of content in the original EDRMS?
- Need to migrate these previous versions?
- Keep only renditions rather than original documents?
- Dispose of any versions or renditions?

Version and rendition risks

The key risk to watch out for is that the receiving EDRM can maintain the document version history needed, associating previous versions with the most recent document. Similarly with renditions, there is a risk that renditions will not be associated with the original document. Need to consider whether the rendition can just be recreated in the new EDRMS (i.e. is it possible to recreate the rendition rather than migrate it?)

Questions to identify risk:

- Can the receiving EDRMS accept multiple previous versions of documents?
- Will it maintain these as version history?
- Will it accept the same number of versions per document?
- Can it migrate renditions of information?
- Will the receiving EDRMS import renditions and appropriately associate them with the original document?

Embedded objects and attachments

The completeness of the information may depend on maintaining embedded or attached objects, for example between an email and its attachments, or between a document and associated charts or graphics.

Questions to identify requirements:

- What information contains linked objects or attachments?
- Is this required to use the information?

Embedded objects and attachments risks

The key risk here is that the receiving EDRMS un-embeds objects, and that links between documents and attachments could be lost if they are not exported/imported.

Questions to identify risk:

- Will embedded objects and attachments be migrated?
- Will links between objects and attachments be maintained?
- If the receiving EDRMS routinely ‘un-embeds’ objects, will this cause issues in how staff understand or use the information?

Links between documents, shortcuts and references

The completeness of the information may rely on maintaining links between documents or objects, related documents, or between a document and external websites and databases.

Similarly, the originating EDRMS may contain references or ‘shortcuts’ to documents in various places within the fileplan, so that the same document can be located and opened from numerous locations and contexts.

Questions to identify requirements:

- Do links between objects in your EDRMS need to be maintained for your information to be complete?
- Can staff understand, use and trust the information without these links?
- Do references and ‘shortcuts’ created within the EDRMS need to be maintained? Are these important for maintaining context and for finding relevant information?

Links between documents, shortcuts and references risks

There is a risk that the EDRMS migration will move content and key metadata between systems, but complex information on how the documents relate to each other and parts of the file plan will not be migrated so successfully. There is no standard way of exporting this information, which is usually created and managed internally as an integral part of the EDRMS functionality in a way that is not designed for import into another system.

Questions to identify risk:

- Will associations and links between documents managed by the EDRMS be maintained on migration, e.g. email and attachments?
- Will links within documents to other sources, e.g. hyperlinks, linked spreadsheets or project plans, be maintained on migration?
- Will aliases/shortcuts to documents within the EDRMS be exported as a copy of the original, or as a shortcut link using internal identifiers? Can the importing system resolve these aliases and create new ones?

Audit trails and logging

Audit trails and other logs capture information about a range of actions relating to the information. For example, how and when it was accessed, amended, published, disclosed or moved and by whom. Maintaining access to audit and logging information may be particularly important if it is important to demonstrate particular trust levels in your information.

Questions to identify requirements:

- What audit trails are captured by the originating EDRMS?

- How long do you need to keep the audit trails?
- Do you need the audit trail information to use, understand or trust the information?
- Do audit trails or logs not held in the EDRMS need to be kept in order to trust the information?

Audit trails and logging risks

The significant risk here is that staff will not be able to effectively export or import audit and logging data required. The contingency for this is to find some way of maintaining the information external to the EDRMS so that it can be referenced if required.

Questions to identify risk:

- Can the audit trails from the EDRMS be migrated?
- Can the receiving EDRMS import audit data and maintain associations with the relevant documents?
- Can audit data be maintained in an accessible way external to the EDRMS for reference?

Availability of the information

Ensuring that the information remains available following migration involves considering how staff will find and access the information and whether the new EDRMS can provide the technology needed to work with it. This includes:

- Search and locations
- Access control
- Encryption and passwords
- File format types

Search and locations

Alongside providing key context and content, metadata can also support finding the information within the EDRMS. An understanding of the metadata and context used to support locating information will inform the migration process.

Questions to identify requirements:

- Do users find information by searching or browsing?
- What metadata fields are most used for locating information?
- What parts of the classification scheme or file plan are used for browsing for information?

Search and locations risks

Many of the risks to finding information following migration relate to maintain its context, through appropriate contextual metadata and location within the file plan or classification structure – as detailed above.

Need to consider the search functionality provided by the receiving EDRM, which may differ or use the information differently. A consideration of the search function at an early stage will inform mapping the metadata schemas and may prompt changes in how metadata fields are migrated, to assist in making the information findable.

Questions to identify risk:

- Will the receiving EDRMS provide the same search functionality?
- Does it support search on the same metadata fields as the originating EDRMS?
- Is it a requirement to map data into different metadata fields to enable finding the information?
- Does the receiving EDRMS support full context searching and will this be addressed as part of the migration process?

Access control

EDRMS may implement access controls to limit who can make use of the information and in what way. These access controls may depend on certain metadata criteria, e.g. author, sensitivity, protective marking.

Questions to identify requirements:

- Will the new EDRMS need to restrict or limit access to information in the same way in future?
- Is access to information currently governed by particular metadata (e.g. author, sensitivity or permissions metadata)?

Access control risks

Different EDRM Systems may define and use access control functions very differently. Some may rely on external authentication, or have inbuilt levels of permissions that will need replicating on the receiving EDRMS to maintain the same controls.

There is a risk that, if not carefully managed, when information is migrated it will not retain the access controls or permissions – resulting in people have inappropriate access to information.

Questions to identify risk:

- What access controls are reliant on to restrict access to the EDRMS and/or documents within it?
- Will the receiving EDRMS be governed by the same access controls and permissions?
- Can permission/access be migrated alongside the information?

- Will the new EDRMS be able to replicate the same level of access control to information as in the old EDRMS?

- Will changes to access controls and permissions to achieve this need to be made?

Encryption and passwords

Information can be encrypted or password protected if it is particularly sensitive, or for transfer to a different organisation. Migrating information between EDRMS is a good opportunity to review whether encryption for information is still required.

Questions to identify requirements:

- Is any of the information encrypted or password protected?

- Should encryption be retained?

- Is password protection required?

Encryption and password risks

Risks may arise from migrating encrypted information if the EDRMS in particular manages encryption or password protection. Need to ensure that the receiving EDRMS can handle encryption, and that information that needs to be password-protected remains so

Questions to identify risk:

- Does the EDRMS contain encrypted information?

- Can the receiving EDRMS handle encrypted information?

- If the information has to be unencrypted, what additional controls will be needed to put in place to maintain information security?

File format types

Some of the ability to use the information as needed will be dependent on particular file formats, for example a spreadsheet that needs certain formulae or macros to be understood and used correctly.

Questions to identify requirements:

- What file formats is the information held in?

- Does the usability of the information depend on features of a particular file format?

File format risks

There is a risk that the information being migrated will contain information types or formats that cannot be handled by the receiving EDRMS. Or, that these file formats will be handled differently. Or that there are file size limitations in the receiving EDRMS that affects its ability to handle certain information or formats.

For example, older EDRMS may not recognise modern Office document formats such as .docx, impacting on the user’s ability to directly open these documents in the appropriate software.

As well as considering whether the EDRMS itself can handle the relevant file formats, there is a risk that transferring information to another system, staff may not have the technology needed to access the information. This risk increases if the EDRMS contains old, specialist or unusual formats less likely to be in use in the receiving system.

Questions to identify risk:

- Can the receiving EDRMS handle the same range of file formats and does it handle them in the same way?
- Are there file formats that the receiving EDRMS will not recognise or cannot accept?
- Can the receiving organisation support the file format types being migrated?
- Are there file format types being migrated for which there is no technology available to open and use the information as needed

REFERENCE:-

Migrating Information between EDRMS by the National Archives, London

This guidance is published by the Digital Continuity Project and is available from www.nationalarchives.gov.uk/dc-guidance