The National Archives

Migrating information between records management systems

This guidance relates to:
Stage 1: Plan for action
Stage 2: Define your digital continuity requirements
Stage 3: Assess and manage risks to digital continuity
Stage 4: Maintain digital continuity

This guidance should be read **before** you start to manage digital continuity. The full suite of guidance is available on The National Archives' website.

This publication is available for download at nationalarchives.gov.uk.

Contents

1 Introduction

Digital continuity is the ability to use your information in the way you need, for as long as you need.

Digital continuity is put at risk by change – including changes to how you use and manage your information, the organisational structures that govern it, and the technology used to access it. You need to manage your information carefully over time and through change to maintain the usability you need.

1.1 What is the purpose of this guidance?

This guidance will help you prepare for migrating information between record management systems. For the purpose of this document this could be the migration between Electronic Document and Record Management Systems (EDRMS), Enterprise Content Management (ECM) or Content Management Systems (CMS), or from one to the other. It focuses on maintaining the continuity of your information.

Note: all records management systems will be referred to as EDRMS for simplicity.

This guidance will help you to understand:

- why migrating information between EDRMS poses risks to your digital continuity
- how to define your information and migration requirements
- key risks to digital continuity to watch out for when 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 system
- provide detail on every aspect of managing a system 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.

If you are reading this guidance, we assume that it is because you have an EDRMS and have identified a potential need to migrate information from that system into another EDRMS. This may be due to changes in your organisation (for example, transferring information to another organisation with a separate EDRMS), or may be due to changes in technology within your organisation (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 types and formats. Although aimed primarily at system migrations, many of the planning principles and risks could apply to general data migration projects.

This document forms part of a larger suite of guidance produced by The National Archives relating to digital continuity.

1.2 Who is this guidance for?

This guidance is aimed at someone leading or managing a project to migrate information between EDRMS such as a project manager or someone from an information management or IT function. The guidance may also be useful to 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 their 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 Why does system migration pose a risk to maintaining digital continuity?

EDRMS provide complex mechanisms and structures for organising and providing access to information. Different EDRMS 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 that you will lose some or all of the information content or context, or your ability to access it, so that you can't:

- **find** the information you need
- **open** the information you need
- **work with** your information in the way you need
- **understand** what your information is, or what it is about
- **trust** your information is what you say it is

System migration therefore requires careful planning and management to ensure that you:

- understand how you need to use your information
- ensure that you maintain the completeness, availability, and therefore usability of your information throughout the migration process
- manage the risks involved in migrating your information between EDRMS

You should also use it as an opportunity to ensure that the EDRMS you are migrating information into has the properties you need to ensure digital continuity – such as capability to import and export information effectively, facilitating further changes in the future.

3 Preparing for successful migration between EDRMS

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

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

Risks increase when system 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 IT, information management, information assurance and business management. For example there's a risk if the migration is an IT-led technical exercise that does not sufficiently engage with the business requirements for information. Conversely, there will be increased risks and issues if IT 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 system migration can incur significant costs, both in terms of resources and expenditure for specialist expertise and supplier action. You can only justify these costs by being sure that migration is the right route for you in the first instance. Managing the project carefully with detailed planning and testing will reduce risks, issues and unnecessary cost increases.

Before undertaking a migration you need to consider if migration is the right response? Are there alternatives that should be considered at less cost and risk that still meet business need? See section 5.2 for more on alternatives.

3.1 Key principles for managing your system migration

System migration is more likely to succeed if you follow these six key principles:

1. Manage it as a project: establish a strong project structure and management process to deliver the system migration. Include expert project management support and project governance that is tied in to the business and owned at the appropriate level. This is critical even if the migration is being primarily handled by external IT providers – you will still need to assure and lead their delivery. 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 (see section 4).

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

3. Involve the right expertise: you need to ensure you involve the right people with the right skills, including people who understand the business requirement, and those who understand the technology and information structures. A cross-disciplinary project team involving staff from information management, IT and information assurance functions would be ideal. If relevant, you also need to ensure your suppliers are deploying the right skills to support this work.

4. Lead with business requirements/user needs: understand the outcomes you are trying to achieve, namely how the business needs to use the information you plan to migrate. You need to ensure ownership of the requirements at the appropriate levels – for instance, Information Asset Owners (IAOs), Chief Executive (CEO) or heads of the business units that depend on the information. This will help you decide what, when and how to migrate; ensuring you get the results you need and maintain your digital continuity in the process (see section 5).

5. Manage risks carefully: system migration poses a risk to your digital continuity, so you need to have the right risk assessment processes in place. Make identifying and controlling risk a key part of how you manage your migration project. You should ensure ownership of the risks at an appropriate level (including the business risk of information not being fully usable following migration) – most likely you will involve someone at executive level, such as a CEO. This will help you to identify risks in advance and avoid or mitigate them before issues arise (see section 6).

6. Test for continuity: frequent and extensive testing prior to and following the migration will help ensure you address issues before they arise. You can then move confidently to using the new EDRMS and disposing of the old one (see section 7).

4 Managing your migration project

4.1 Migration project stages

Following good project management principles is critical to ensuring a successful system migration project. The type of project you will need to establish will depend, in part, on your drivers for considering migrating information between EDRMS. If you are moving information from one system into another already established one, for example prompted by a Machinery of Government (MoG) change, then the project can focus mainly on migrating the information safely. If you are implementing a new EDRMS and plan to move information from a pre-existing system into the new one, then you will need to integrate the information migration component into the organisation's wider EDRMS implementation programme. You will also need to follow your organisation's existing change and project management processes.

Our accompanying *Project checklist for records management system migration* contains a checklist of key components at each stage that you can use to help manage your project.

4.2 Responsibilities and expertise involved

To ensure you manage digital continuity, your project team will require access to a range of capabilities to support the various stages of the migration process. Capabilities are listed below. In practice the necessary skills may not reside with a single individual, or several areas of capability may be combined in one role. The precise make-up of your project team will depend on the size, complexity and risk of your migration project.

Capability	Why it matters
Project management	Overall management of the process, reporting, delivery against the required outcomes. It is recommended that you use an Agile approach to project management to build and run government digital services. Agile methods encourage teams to build quickly, test what they've built and iterate their work based on regular feedback. See the gov.uk service manual for a wide range of guidance and community support. Using Agile methods will have a direct impact on capabilities such as risk management, testing and communication.

Business analysis	How the business needs to use its information. Will draw on expertise within business units and needs to understand the legislative environment, involving specialists in data protection, freedom of information, record management, information assurance and so on.
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.
Communications	Communication with the receiving organisation (in case of MoG change). Internal communications (in case of IT change). Communication of any impact of change on the business.
Contract/supplier management	Liaison with IT suppliers (service providers, software vendors, implementation partners, specialist IT services). Understanding service levels and managing costs.
Testing	Testing of processes. Testing whether migrated information continues to meet requirements (see section 7).
Information architecture and/or data migration expertise	Developing the migration process. System administration, schema design and interpretation, data transformation, export/import mechanisms, secure transfer, decommissioning and disposal.
Information assurance, security and access control	Identify and manage any information assurance risks and security processes. Establish required access control.
Information governance (FOI, DPA leads)	Inform requirements and testing to ensure compliance with relevant policies and legislation.

4.3 Managing single or multiple third-party suppliers

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

When procuring new or existing services, public sector organisations should consider and fully evaluate potential cloud and on premise solutions to ensure this supports the value for money. This approach is mandatory for central government and strongly recommended to the wider public sector.

For more information see the Technology Code of Practice guidance and the G-cloud framework on gov.uk.

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

If your system migration is being managed for you by your suppliers, we recommend the following 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 you do not have the in-house expertise to assure their plans
- Ask your suppliers to detail how they are going to meet your requirements prior to the migration, to enable you to assure their process and confirm it is likely to meet your needs. Request detail on the schema mapping and procedures for migration
- Ensure that your suppliers contribute to risk and issue management, and share with you their assessments of the risks and issues associated with your migration, and their plans for managing these
- Ensure that where multiple suppliers are involved in a migration that you facilitate communication and coordination 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 coordination 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. You may need to clarify who is the lead supplier for the migration project, and hence

responsible for managing the coordination 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 your business requirements for the information you are considering migrating between EDRMS is the critical first step. You must do this before planning or undertaking a migration. You will need to identify the following:

- What information the originating EDRMS holds – and what may need migrating
- How the business needs to use the information (see section 5.1)
- Whether migration is the right response (see section 5.2)
- What information you are migrating (see section 5.3)
- How to maintain the digital continuity you need through the migration (see section 5.4)

5.1 Define what information is affected and how you need to use it

Before you start down the path of system migration, you need 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 you need to achieve. This will help inform whether migration is the right approach, and shape the migration process itself.

The overall aim of a system migration is to enable business and operational continuity by ensuring that the information remains available and usable to 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, you do not need to identify very detailed requirements. You just need to understand enough about your information to decide whether migrating the information between EDRMS is necessary.

Questions you need to ask include:

- Do you still need regular access to the information?
- If so, who needs access and how readily?
- 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 you 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?
- 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? If so, for how long?

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 system migration is the right approach

A high-level understanding of your information means you will be in a position to confirm if migrating the information between EDRMS is the right approach to take.

System migration is a costly, risky and complex exercise and should not be undertaken until you are sure of the business need. You can then do a reasonable cost-benefit analysis of whether the projected costs and risks of migration are justified by the business need and benefits from having the information in a different EDRMS.

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

Alternatives to system 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.

With the originating organisation: If system migration is being considered following a MoG change, the originating department may be able to continue holding the information as a service to the receiving organisation. Although no physical migration would occur, ownership of, and responsibility for, the information would transfer to the receiving organisation. The precise rights and responsibilities of each organisation would need to be established.

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 – you may want to migrate it from the EDRMS to a more suitable platform. 'Archive' environments generally offer some of the features of an EDRMS (i.e. hold structured content associated with descriptive information) though often with reduced functionality, lower performance, and lower cost.

At The National Archives: It may be appropriate to consider transfer to The National Archives under certain circumstances. For example if the information is no longer in active business use, has been selected for permanent preservation, meets the technical requirements for transfer and has undergone sensitivity review.

For more information on transferring digital material to The National Archives see our guidance steps on Digital records transfer.

5.2.3 Disposing of information

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

For more information see our guidance on Disposing of records.

5.3 Identify what to migrate

If system migration is the right approach to meet your business needs, you must decide whether to migrate all the content of the EDRMS, or just some of it. If it is only a partial transfer, can you clearly identify which information you need? Do you have a strategy for disposing of the information you are not migrating, as appropriate?

Examples of what to consider when migrating information:

- available formats (xml, csv, tsv, proprietary)
- available methods (archival, disposal, full part, bulk, batch, manual)
- levels covered (classes, folders, sub-folders, parts, records, components)
- objects/documents covered (draft, finalised, declared, corporate value)
- custom fields covered
- user profiles (access, security)
- role definitions (functional rights, privileges)
- disposal schedules
- audit trail data

- function-related data
- workflow definitions

5.4 Define detailed digital continuity requirements

You now have a high level understanding of how your business needs to use information. The final critical stage is to turn these into more detailed digital continuity requirements for the information you plan to migrate. This will require you to define how you need your information to be complete, available and therefore usable following the migration. Use this statement of requirements to plan, assure and test the migration process to make sure you have maintained the information use you need.

Note: this is not the same as specifying system requirements. You should focus on the features of your information that you need to maintain, rather than the functionality of the technology. How you need to use your information will inform how you specify and configure the receiving EDRMS, and the functionality you need from a new system.

You need to identify what you require of your information for it 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)

Again, you should refer to your organisation's IAR or similar list. You should liaise with your information management team and relevant IAOs to make sure this information is correct and up to date and agree any changes to usability requirements that you identify as part of this migration process.

Depending on the type of information held in your EDRMS you will need to consider the best level of detail at which to define your requirements. For example, you may define:

- a generic set of requirements for all information to be migrated
- a varying set of requirements for the information which supports a particular business need
- 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 you need to ask to produce detailed requirements, see the Appendix.

5.4.1 Completeness

What content, context and provenance information do you need so that you can use your information as required?

- **Content**
  Content is the core information found within the EDRMS. Once you have identified the different document types and formats you want to migrate, you need to consider what aspects of the content you need. What metadata, version histories, renditions and embedded objects and attachments do you require 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 you to find, work with, understand and trust your information. Context can be provided through a number of different sources. You need to identify what contextual components to migrate alongside your content, and how you will maintain the crucial link between the two. 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 your 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

You will need to consider whether you 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

What do you need in order to be able to find, open and work with information as you need to, 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 you plan to manage encrypted or password protected information. Identify what file formats the information to be migrated is held in.

The National Archives has developed a free software tool, DROID, to help you to automatically profile a wide range of file formats. For example, it will tell you what versions you have, their age and size, and when they were last changed. It can also provide you with data to help you find duplicates.

5.5 How to use your business continuity requirements

Once you understand your digital continuity requirements, you will be better placed to manage and plan moving the information from one system to another. You will have identified the key components of the information held in the EDRMS, which, alongside the content, will need to be in place in the new system to enable the usability you require.

You can now use these requirements to do the following:

5.5.1 Communicate your usability requirements to the wider project team

This can help to ensure that everyone working on the project has a shared understanding of what you need to achieve through the migration.

5.5.2 Specify the functionality you need from a new EDRMS

Your understanding of what must be transferred from the old to the new will help you to specify detailed 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 your requirements

If there are technical, financial or business constraints on your system migration project, you may need to compromise what requirements you meet and how. By having a detailed picture of your requirements, you will be able to have an informed 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

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

If you are selecting a new EDRMS, ensure that the system you are procuring and migrating to has good continuity properties (for example, good import and export facilities). This will enable you to minimise migration issues and risks to the continuity of your information in future.

6 Managing key risks and issues

System migration carries many risks and the success of the project can depend on careful risk management. You need to understand up front the business impact of not being able to use the information in the way you need during and following the migration – and ensure that the business is aware of these risks. If you are transferring information between organisations, for example after a MoG change, it is important that you consider the requirements, risks and business impact on both organisations.

Consider such risks as:

- security risks relating to cloud solutions (see section 4.3). The National Cyber Security Centre provides useful guidance on implementing cloud security principles – Principle 1 deals with data in transition protection
- 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 that you should look out for. Many of these relate to comparing how the two systems handle and interpret the information and its use and access, so that you can continue to meet your digital continuity needs 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 your requirements.

The rest of this section focuses on the key risks to digital continuity:

- understanding your 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

If you do not understand your information requirements thoroughly, you may not realise that the migration does not provide what you need until it is too late.

EDRMS are all different and rarely present and handle information in the same way, so you may have to make compromises in requirements. Identify what requirements are business critical, and which are only desirable, to help you prioritise. You may also choose to reduce the scope of your requirements, for example prioritising the ability to find and understand information inherited from another organisation needed for audit or accountability purposes only.

6.2 Constraints in the technical capability of the EDRMS

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

If you face constraints over what EDRMS you are migrating information into, you have to manage an increased number of issues and risks. For example, if the migration is due to a change in organisational structures and the receiving EDRMS is a pre-existing system belonging to another organisation, this system might not meet all of your requirements and you may have to make compromises.

In particular, in order to plan the migration and assess risks effectively, you will first 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 you will need to undertake to ensure that the metadata, content and associations can be transferred between the two systems. Based on this understanding, you may need to refine and revise your requirements. 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 you will lose key information, 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.

You may need to talk to your EDRMS suppliers to understand the import/export functions available. Even when an export function is available, it is rare that an EDRMS export captures everything held in the system,

so you may have to make informed compromises. Similarly, the import functionality on the receiving EDRMS may not be able to handle all the information you want to migrate.

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? Do you know how the metadata is 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. You can find more information on the risks associated with metadata in the Appendix.

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 EDRMS 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?

6.3 Updating information governance and business process

6.3.1 Information governance and ownership

As the migration carries significant risk, you will need to ensure that you engage the appropriate information governance structures and accountable staff such as IAOs. Provide visibility of the project and risks at the right level, including up to the CEO if your EDRMS contains business critical, personal or sensitive information.

You need to establish clear owners for the information before and after migration. It is particularly important that you ensure information is transferred appropriately if the system migration is due to changes in your organisation structure, such as a MoG change. 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

You need to identify whether you need to make any changes to the business process for managing information subject to migration, to meet your requirements. By introducing a different EDRMS, and potentially moving information into a different organisation, it is likely you will need to adopt different business processes. 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 system migration

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

Refer back to the requirements and acceptance criteria you defined and develop acceptance testing processes that fully test whether each requirement has been met. Our *Testing for Continuity Checklist* might be a useful guide to help shape your acceptance testing and ensure that you have maintained continuity.

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

Once you are confident that the migration has been a success, you can dispose of the information held in the originating EDRMS and decommission the system, if appropriate. If there is information that it was not possible to migrate successfully, you may want to retain the originating EDRMS for a period to migrate or otherwise manage access to this information as you need – 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.

Appendix

This section provides further detail on the key areas you should consider when defining your requirements from system migration, and indicates additional potential risks to watch out for in meeting those requirements. This section should be read in conjunction with the high-level technical capability risks outlined in section 6.2.

Completeness of your information

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

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 be 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 do you need in order to find, use, understand and trust the information? e.g. metadata about:
  - roles (author, owner, editor, contributors, etc.)
  - dates (dates created, modified, published)
  - source and rights (owner, source organisation, etc.)
- What existing metadata do you need 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 you 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, you need 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, for example 'date', 'author' may be used differently, and change the apparent meaning of the information for the user. You need to understand how the receiving EDRMS interprets and displays its metadata before you decide how to map your 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. You must undertake extensive testing to ensure you maintain the completeness of your information when migrating metadata.

Questions to identify risk:

- Can the critical metadata fields be exported/imported?
- Do the metadata schemas of the two systems align?
- Are there places in the receiving metadata schema that you can map all the metadata you need to?
- 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 titled 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, you need to ensure that this contextual folder structure can be migrated alongside the content and metadata.

Questions to identify requirements:

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

Conversely, if you want to integrate the information into the receiving file plan, map each area of the source classification scheme to its equivalent in the destination classification scheme – which you may need to amend 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/file plan structure be migrated?
- Does the import/export function maintain location within the file plan?
- Is your 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. You may or may not need these.

A rendition is an instance of a record rendered into another software format, (for example, 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?
- Will you need to refer back to these versions or do you need to keep them for audit purposes?
- Do you need to access and use renditions of content in the original EDRMS?
- Do you need to migrate these previous versions?
- Do you want to keep only renditions rather than original documents?
- Can you dispose of any versions or renditions?

Version and rendition risks

The key risk to watch out for is that the receiving EDRMS can maintain the document version history you need, 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.

You should 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 you 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 your 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:

- Do you know what information contains linked objects or attachments?
- Do you need to retain these 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 you understand or use the information?

Links between documents, shortcuts and references

The completeness of your 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 you need to maintain links between objects in your EDRMS for your information to be complete?
- Can you understand, use and trust the information without these links?
- Do you need to maintain references and 'shortcuts' created within the EDRMS? Are these important for maintaining context and for finding relevant information?

Links between documents, shortcuts and references risks

There is a risk that the system migration will move content and key metadata between EDRMS, 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 you need 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 the audit trails form part of your forensic readiness plan, e.g. do they provide evidence that you might need in future?
- Do you need the audit trail information to use, understand or trust your information?
- Do you need audit trails or logs not held in the EDRMS in order to trust the information?

Audit trails and logging risks

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

Ensuring that your information remains available following migration involves considering how you will find and access the information and whether you can provide the technology you need to work with it. This includes:

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 associated with finding information following migration relate to maintaining its context, through appropriate contextual metadata and location within the file plan or classification structure – as detailed above.

In addition, you need to consider the search functionality provided by the receiving EDRMS, 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?
- Do you need 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:

- Do you 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 EDRMS 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 you will not retain the access controls or permissions – resulting in people having inappropriate access to information.

Questions to identify risk:

- What access controls are you 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 you migrate permission/access alongside the information?
- Will you be able to replicate the same level of access control to information in the receiving EDRMS?
- Will you need to make changes to access controls and permissions to achieve this?

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?
- Do you need to retain this encryption?
- Do you need password protection?

Encryption and password risks

Risks may arise from migrating encrypted information if the EDRMS in particular manages encryption or password protection. You will 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 you need to put in place to maintain information security?

File format types

Some of your ability to use the information as needed will be dependent on particular file formats (see (section 5.4.2), for example a spreadsheet that needs certain formulae or macros to be understood and used correctly.

Questions to identify requirements:

- What file formats are your 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 if you are transferring information to another organisation, you 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 organisation.

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?