The National Archives

Identifying Information Assets and Business Requirements

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 has been produced by the Digital Continuity Project and is available from www.nationalarchives.gov.uk/dc-guidance

Any enquiries regarding the content of this document should be sent to digitalcontinuity@nationalarchives.gsi.gov.uk

Contents

1 Introduction

How much digital information does your organisation hold? Who takes care of it?

The amount of information organisations create is continually increasing, and whether your organisation is large or small, if you do not understand your information, you cannot fully protect and exploit it. This guidance describes a practical process to enable you to understand, assess and document your information and make sure that it supports your business appropriately.

1.1 What is the purpose of this guidance?

This piece of guidance focusses on understanding the information your organisation holds and how it needs to be used to support your business. Developing this understanding will support you in effectively managing your information assets through change.

This guidance will enable you to:

- understand your business drivers for this investigation and frame your objectives accordingly
- identify your information assets
- understand your business requirements for using information
- document the relationships between your business requirements and your information assets in a way that supports your objectives.

The reasons, or 'drivers', for undertaking this investigation can vary and therefore lead to varied scopes and objectives, from large scale audits of all of your organisation's information, to very focussed assessments for a specific change in technology or business.

Regardless of what your drivers are for carrying out this study, there are multiple benefits which can have a wider reaching impact than your original scope. These include better change management, improved understanding of information risk and identification of potential savings and efficiencies.

1.2 Helping you manage digital continuity

Although this guidance contributes to overall good information management and can be used to meet a number of different objectives, one of the key objectives it supports is better management of your digital continuity.

Digital continuity is the ability to use your information in the way you need, for as long as you need. Managing digital continuity protects the information you need to do business. This enables you to operate accountably, legally, effectively and efficiently. It helps you to protect your reputation, make informed decisions, avoid and reduce costs, and deliver better public services. If you lose information because you haven't managed your digital continuity properly, the consequences can be as serious as those of any other information loss.

This guidance forms part of a suite of guidance[1] that The National Archives has delivered as part of a digital continuity service for government, in consultation with central government departments. This specific piece provides you with practical information and support to help you complete Stage 2 of the four-stage process of managing digital continuity.[2] Stage 2 is all about understanding your business requirements for information use and how your information assets and technical environment support those requirements, now and in the future. This knowledge can then be used to perform a risk assessment and then take action – establishing processes, making savings and efficiencies and minimising your risk.

We suggest breaking this process into two halves. The first half of this process (identifying your information assets and mapping them to your business requirements) is covered in this piece of guidance. An accompanying piece of guidance, *Mapping the Technical Dependencies of Information Assets*[3] covers the second half of this process.

1.3 Who is this guidance for?

The audience for this piece of guidance will vary depending on the drivers for performing the investigation. For digital continuity, the primary audience will be the Senior Responsible Owner (SRO) and whoever the SRO has assigned to be responsible for completing Stage 2

[1] For more information and guidance, visit nationalarchives.gov.uk/dc-service
[2] See *Managing Digital Continuity* nationalarchives.gov.uk/documents/information-management/managing-digital-continuity.pdf
[3] See *Mapping the Technical Dependencies of Information Assets* nationalarchives.gov.uk/dc-guidance.

of the process. If the driver is to perform an impact study for a potential change, then it may be a change or project manager using this guidance.

Regardless of their role, the person leading the process will likely have to consult other members of the organisation who may also find it useful to read this piece to understand the background – for example business continuity managers, Information Asset Owners, IT professionals and business analysts.

2. Setting your objectives

You need to be very clear about why you are looking at your information, what your reasons are for starting the investigation and what you hope to achieve from it. Your own driver may be reactive – an incident has occurred (for example a badly managed change, or a loss of data) and you want to ensure it does not happen again. On the other hand, the driver may be more preventative – your organisation is preparing to go through a specific change (business or technical) and you want to make sure you have the necessary understanding to best protect your digital information.

These different drivers will give you different objectives, and will therefore direct the scale and scope of your investigation. For example, do you need to do this evaluation for your entire organisation, or just for a discrete business unit within it?

While it is important to eventually review all your information, unless you are a small organisation with a relatively low amount of digital information, trying to capture everything in detail at once is likely to be an overwhelming task. It is far better to have realistic objectives prioritising key areas you want to look at, and focus on other areas later.

You must ask yourself questions about what you are trying to achieve and what your priorities should be – what do you want to do with the information you are going to gather, what can you practically achieve, what risks do you need to mitigate, what benefits do you hope to achieve, and what areas need the most urgent attention?

The following sections 2.1-2.6 give examples of some high-level objectives:

2.1 Managing digital continuity

"We want to better manage the digital continuity of our information – so that we can use it in the way we need to over time."

If you are working through the four stages of the managing digital continuity process, establishing your scope and priorities is an important part of Stage 1 and is covered in more detail in *Managing Digital Continuity*.[4]

[4] See *Managing Digital Continuity* nationalarchives.gov.uk/documents/information-management/managing-digital-continuity.pdf

However, even if you are not specifically working through the four stages of that process, better understanding of your assets and their requirements will automatically improve your digital continuity. You have digital continuity if your information is complete, available and therefore usable in the way you need it to be. To manage your digital continuity, you must first understand your business requirements, how you need to use your information to meet those requirements and what functionality your technology environment needs to provide.

2.2 Change management

"Our organisation is planning a change and we want to make sure we understand what information we have, and how to manage it through the transition."

It may be that a driver for this work is that your organisation is going through a change, either an organisational one such as a restructuring, or a technological one such as upgrading a key system. It may also be that there is no specific change at the moment, but you want to introduce or improve a change management process and be prepared for the future.

Change is a major threat to your information (it is the key risk to digital continuity) and an important time to consider what information assets you actually have and how you can protect and exploit them. During change it is very easy for things to move out of alignment, for technology to stop supporting the use of your assets in the way that you need, or your information assets to fail to provide the data that new business requirements call for.

2.3 Managing risks and improving governance

"Our organisation wants to better understand risks and mitigate them through improved governance and processes."

This work will allow you to better understand how to manage your information and how to mitigate risks. You may opt to look at a subset of risks (e.g. risks to digital continuity or information security, or risks arising from change) or risks to specific areas of information.

The specific risks you look at may depend on your risk appetite, for example risks to information which is business critical are likely to be a priority. It is important to understand your obligations – for example in regards to the Data Protection Act, or confidentiality requirements where you may incur penalties if problems occur.

2.4 Managing retention and disposal

"Our organisation wants to audit our information so we know what we need to keep, how we can store it efficiently and what we can dispose of."

Digital information is being created at an ever-increasing rate, and this can lead to rising data storage costs and more and more difficulty in finding information. It is becoming ever more important to carefully consider what you need to keep and how you need to be able to access it.[5] Understanding this allows you to define retention schedules and safe processes for disposal. This can lead to reductions in the amount of storage required, leading to cost efficiencies and contributing to green agendas.

2.5 Exploiting and sharing information

"Our organisation wants to understand what information we can share and how we can do it."

The government agenda on transparency makes it very clear that opening data up is a key priority wherever possible. In order to best exploit and share your information both within your own organisation, between related organisations and with the wider public, it is vital you first understand your information. Going through this process will put you in a position where you fully understand what information you have and what you can and cannot do with it. This will also allow you to respond more easily and quickly to requests for information.

2.6 Streamlining technology

"Our organisation wants to better understand our technology systems and whether we can streamline them without losing functionality."

Once you have evaluated your information assets, you can map them to the technology support they need. If you perform a comprehensive audit, you will confidently be able to identify surplus technology which could be decommissioned leading to savings. This process is covered in *Mapping the Technical Dependencies of Information Assets.*[6]

[5] See 'What to keep' guidance on The National Archives website nationalarchives.gov.uk/information-management/projects-and-work/what-to-keep.htm
[6] See *Mapping the Technical Dependencies of Information Assets* nationalarchives.gov.uk/documents/information-management/mapping-technical-dependencies.pdf

3. Identify what information assets you have

3.1 What is an information asset?

In order to understand your information and how to manage and protect it, it is vital to first understand what we mean by the term 'information asset' and how this definition can simplify the process.

> **An information asset is** a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively.
>
> Information assets have recognisable and manageable value, risk, content and lifecycles.

The key concept here is to group your individual pieces of information into manageable portions; if you had to individually assess every individual file, database entry and piece of data you hold you would likely have a list of millions of items and an impossible task. By grouping items at a level to match your objectives you can make the task actually achievable.

3.2 How do you identify an information asset?

You should identify your assets according to the definitions above, considering the level of granularity that is required to meet your objectives. An information asset is defined at a level of detail that allows its constituent parts to be managed usefully as a single unit.

The case studies in the Appendix provide some examples of how different objectives can be met by varying the granularity of your information assets.

To perform this audit, you will need to talk to representatives from all sections of your organisation to ensure you have covered all aspects of your business. Your organisation may already have resources you can use to help in this process, for example documentation of previous information audits, technical environment registers, configuration management databases or software asset lists. You may also have Information Asset Owners (IAOs), a role which was identified by the Data Handling Review and mandated by the Cabinet Office.[7]

[7] Cabinet Office Guidance on the Mandatory Role of the IAO www.cabinetoffice.gov.uk/media/204709/iao_role.pdf and The National Archives' guidance nationalarchives.gov.uk/documents/information-management/role-of-the-iao.pdf

You should investigate these resources and re-use and adapt them wherever possible. However they may only be a very basic foundation to start from and there will almost certainly be additional information you will need to gather.

It is probably easiest to start with very broad definitions and then continue splitting the information grouping up until it is of a suitable size. To assess whether something is an information asset, ask the following questions:

- Does it have a value to the organisation? Will it cost money to reacquire the information? Would there be legal, reputational or financial repercussions if you couldn't produce the information on request? Would it have an effect on operational efficiency if you could not access the information easily? Would there be consequences of not having this information?
- Is there a risk associated with the information? Is there a risk of losing the information? A risk that the information is not accurate? A risk that someone may try to tamper with it? A risk arising from inappropriate disclosure?
- Does the group of information have a specific content? Do you understand what it is and what it is for? Does it include all the context associated with the information?
- Does the information have a manageable lifecycle? Were all the components created for a common purpose? Will they be disposed of in the same way and according to the same rules?

Examples: Information asset
A database of contacts is a clear example of a single information asset. Each entry in the database does not need to be treated individually; the collection of pieces of data can therefore be considered one information asset. All the pieces of information within the asset will have similar risks associated with privacy and storage of personal information.
All files associated with a specific project may be considered a single information asset. This might include spreadsheets, documents, images, emails to and from project staff and any other form of records. All the individual items can be gathered together and treated the same as they have similar definable content, and the same value, business risk and lifecycle.
Depending on the size of your organisation, you may be able to treat all the content in your electronic document and records management system as a single asset – but this could be a risk as such a large asset containing varied types of content is likely to be hard to manage.
All the financial data for an organisation could be considered a single asset. There are very specific risks to the business if this information is mismanaged and you may also have an obligation to provide transparency of information, which could be problematic.

Note:

- Information assets should be grouped and considered depending on their business needs **not** on their technology requirements. Each asset may contain individual items that need different technology solutions to address the same business need.

- It may be that a piece of information could logically belong within two different assets, however this can lead to conflicts of ownership and control, so ideally each piece of information should only be included within in a single asset. However assets can reference other assets and care should be taken to manage these potentially complex relationships.

- Assets can contain other assets – as you introduce more and more granularity, it may be useful to retain the sense of the high-level assets. Your organisation must define clear rules about how the management and retention schedules of these assets operate at these different levels.

- The groupings of information within assets may change over time. For example, you may have an asset which contains all the items archived into long term storage, therefore other pieces of information will be added into this asset over time.

This can be a complicated process, but done properly can be of real, lasting benefit to your organisation. There is no right or wrong way to group your assets. The key point to remember is that you are doing all of this within the scope defined by your objectives and if the list you produce is consistent and relevant, then it meets your objectives.

4. Identify how you need to use your information

Once you have identified your information assets, you must determine how you need to use each of them. This covers everything from how you find it, through how you access it to what you do with it. You must also consider any surrounding or supporting information which is important. We have broken this down into five questions you will need to answer:

1) How will you **find** the information?
2) Who can **open** the information and how?
3) How do you need to be able to **work with** the information?
4) What do you need to be able to **understand** about your information?
5) To what extent do you need to **trust** that your information is what it claims to be?

For each of these issues you must consider what the requirements are at the moment, and how they might change over time. This will encompass the retention schedules imposed on your assets – how long do you need them for?

These questions also form the core of digital continuity – what usability you need to maintain for your information over time and through change. If you lose the ability to find, open, work with, understand and trust your information in the way that you need, you have lost its digital continuity.

Note it is possible that in defining these requirements you may want or need to re-define your information assets – this may well be an iterative process. If the contents of your asset have dramatically different requirements in any of these areas, you may need to further subdivide your assets.

4.1 How will you find the information?

The granularity and depth of the search required will depend on the type of asset; it may involve finding the asset itself, searching within the asset for files, or searching within those files to find specific pieces of data.

Examples of requirements:

- It must be possible to find generic information from the system without referencing specific names, in order to meet privacy requirements.
- It must be possible to search within the asset to find files created within a specific date range.
- Any requests for information from the system will always be requested through a system engineer, non-experts will not need to search within it.

It is important to consider these requirements because they impact upon how you store the asset and any technology used for searching and indexing.

4.2 Who can open the information and how?

These requirements cover not only the security issues around people gaining access to restricted or private information, but also the opportunities for sharing information internally and more widely.

Examples of requirements:

- The individual files inside the asset are private and only the person that created the file should be able to open it.
- Everything within the asset is protectively marked, only those with the right clearance should be able to open it.
- The information within the asset should be published openly.
- It must be possible to release individual items inside the asset within 20 working days of a request.

The benefits of ensuring the security of your information is protected are obvious. However, by considering the additional aspects of sharing you will be well placed to meet your targets under the government's agenda on transparency, improving the efficiency of storage, and potentially even reducing the likelihood of duplication of work between and within departments.

4.3 How do you need to be able to work with the information?

This is where you define the functionality that you require from your information assets, how you use them and what you need them to do. This area may overlap with the open

requirements in that there may be different groups of users who need to access the assets in different ways.

Examples of requirements:

- The information must be editable (this may involve using original source files)
- The information must be available for disabled users, in formats suitable for screen readers, for example.
- The creator of the document must have full write access. Everyone else should have read-only access.
- The formulae and functions inside the information must be maintained so they can be updated. It is not sufficient to only be able to access the data.

These requirements describe the functionality that your technology must provide, so by understanding these features you may be able to streamline your software.

4.4 What do you need to be able to understand about the information?

This is about understanding the content and context of your information asset. This additional information is not necessarily included within the asset itself but is vital to making the asset usable. The information may be stored digitally as metadata, but it may also be specific knowledge held by individuals, which may involve training or handover procedures if staff change.

Examples of requirements:

- The information within this asset contains references and links to the content of another named information asset.
- The asset is a large collection of files which must be kept within the current structure, flattening the file structure would confuse the meaning of the files.
- The information asset was created under a specific set of circumstances which must be recorded.
- There is a complex version history which must be maintained, it should be possible to access the information as it was at any specified date.

The filing system within the asset is complex, but undocumented, so those filing and retrieving information from within the asset must be trained in how to use it.

These requirements will help you to understand how your assets interact and allow you to ensure they continue to be usable over time.

4.5 To what extent do you need to trust your information is what it claims to be?

The level of trust required of an asset will vary considerably. The majority of your assets may well not require any additional validation – they speak for themselves. However for others you may have to prove they have not been tampered with, or to certify them as created on a specific date.

Examples of requirements:

- All access to the contents of the asset must be recorded.
- Must be able to verify the integrity of a dataset – that nothing has been inserted into it.
- All previous versions of the contents of the asset must be maintained and accessible.

These requirements are particularly important because they cover your legal requirements and there may be serious repercussions if they are not fully understood and implemented.

5. Documenting the relationships between business requirements and information assets

You must store all the information you have gathered about the assets you have defined, listing all the information assets in your organisation, the business requirements they meet, and the additional information which is vital to managing them. Your organisation may already have some form of Information Asset Register (IAR), for example information asset lists, which are required by public sector information policies. You may be able to use one of these as a starting point, but you will likely have to add additional fields.

5.1 Creating or adapting an IAR

The key purpose of the IAR is to document the links between your organisation's information assets and its business requirements. The IAR should be structured so that it is very easy to see what is affected by changes to either of these areas.

In addition to details of how each asset supports your business there are a number of interesting and useful fields which can be recorded for each asset. How many of these you complete may depend on your objectives as covered in Section 2 above.

The way that you build the IAR will depend on the scale of your objectives and the resources you have available. If you want to register hundreds of assets it may be worth creating or purchasing a software tool to record the information in a database. You should check with your IT team to see if they already have a tool available (for example they may already have a configuration management system which you could input into, or extract a report from). If you have a smaller number of assets, or limited resources, it may be viable to record the information in a spreadsheet.[8]

[8] A template IAR is available online at nationalarchives.gov.uk/documents/information-management/iar_template.xls

Examples: Fields on an Information Asset Register	
Description	Brief description of what the asset is More detail on what the components of the asset are
Users	Who created the asset, or where does the asset come from? Who is the Information Asset Owner? Which department holds responsibility for the asset? Who are the stakeholders?
Date	Creation date Date closed (for closed assets) Last date asset register was reviewed/updated
Asset status	Is this asset being actively updated? Has the asset been closed?
Purpose	What part of the business does this asset support? Business risks from or to the asset
Value	What is the value to the business? What would be the cost of replacing the information?
Retention schedule	How long should it be kept in immediate access? What should happen to it when it no longer needs immediate access? What are the disposal requirements?
How do you need to use your asset	How will you **find** the information? Who can **open** the information and how? How do you need to be able to **work with** the information? What do you need to be able to **understand** about your information? To what extent do you need to **prove** your information is what it claims to be?
Risk	What are the risks to the asset? What are the risks to the business from the asset (for example from its loss, corruption or inappropriate access)?

5.2 Identify owners of the information asset

One of the key fields on the IAR is the owner of the asset who is responsible for making sure the asset is meeting its requirements (the IAO), and that risks and opportunities are monitored. The owner need not be the creator, or even the primary user of the asset, but

they must have a good understanding of what the business needs from the asset, and how the asset needs to be able to fulfil those requirements.

The National Archives has produced guidance on the mandated role of the IAO,[9] as well as guidance on the specific responsibilities of an IAO in relation to digital continuity.[10]

5.3 Maintaining and updating the IAR

To sustain the usefulness of the IAR, it is vital to maintain and update it. You should define a permanent owner of the IAR itself (as opposed to information assets described within it) and a maintenance schedule.

When using IARs, it is important to realise they will have an effect beyond the confines of your own organisation. People doing work for your organisation will need to be aware of the IAR, the effect their work has on the IAR and how they will need to interact with the IAR. This could be external personnel working with your data or could be external personnel looking after some of your infrastructure, such as outsourced IT teams. For more information on this, please see our guidance *Digital Continuity in ICT Services Procurement and Contracts.*[11]

[9] See *The Role of the IAO: A Practical Guide* nationalarchives.gov.uk/documents/information-management/role-of-the-iao.pdf
[10] See *Information Asset Owners and Digital Continuity* nationalarchives.gov.uk/documents/information-management/iao-and-digital-continuity.pdf
[11] See *Digital Continuity in ICT Services Procurement and Contracts* nationalarchives.gov.uk/documents/information-management/digital-continuity-in-ict-procurement.pdf

6. Next steps

The IAR provides you with a comprehensive list of the assets that are important to your organisation within the scope of the objectives you have outlined for this investigation. It may be a list of a hundred assets covering your entire organisation, or it may be just a few assets that will be affected by a change you are planning for. Each entry on the register will have all the additional information about the asset that is required to understand how it should be managed so that it delivers the use that the business requires from it.

There are a number of ways you can use this register to identify risks, exploit opportunities and manage change. You should return to your original objectives and take the corresponding next steps.

6.1 Map to technology dependencies

For each information asset it is now possible to assess what technology is required to meet the relevant business needs. This will also allow you to understand the potential impact of change on your assets, and to make informed decisions about where to prioritise investment in ensuring the continued usability of your information. It should also highlight where savings can be made by not maintaining technical support unnecessarily.

This subject is covered in more detail in *Mapping the Technical Dependencies of Information Assets,*[12] and should be done in conjunction with the IT department.

6.2 Understand your information management requirements

Alongside having the right technical tools to support your information requirements, there are likely to be information management processes which need to support the delivery of the requirements. This may mean introducing, updating and enforcing metadata or security policies, or providing relevant training and guidance on how and where to store files.

[12] See *Mapping the Technical Dependencies of Information Assets* nationalarchives.gov.uk/documents/information-management/mapping-technical-dependencies.pdf

6.3 Identify and mitigate risks

Information assets have risks associated with them, risks from losing the assets, having them fall into the wrong hands, getting corrupted or any number of other issues. By considering these risks you will hopefully be able to mitigate against them and form contingency plans. You may need to escalate these risks to appear on departmental or corporate risk registers.

Further information on specific digital continuity risks, including a *Risk Assessment Handbook* and a self-assessment tool, is now available from the National Archives.[13]

6.4 Identify opportunities for disposal, exploitation, savings and efficiencies

In assessing the business requirements for your information assets, you may have uncovered assets which are no longer actually required and action should be taken to dispose of these. You may also have found that some information assets are only needed very rarely and could therefore be moved to cheaper long-term storage which is less instantly accessible.

If you have identified assets that can, or should be shared, you can begin the process of allowing and promoting this access.

6.5 Manage change

Now that you have a comprehensive assessment of your current information assets and their requirements you are in a much better place to assess how any change may affect them. These changes could be to the assets themselves, how they are managed, the technology supporting them; or the business requirements driving them.

For specific changes you will be able to build impact and risk assessments allowing you to mitigating action and plan contingencies. You can also use this information to improve your change management process to make all future change planning better. It is important to remember that you must embed the management of the IAR itself within your change processes – if the IAR is not kept up to date through change it becomes redundant and misleading.

[13] See the risk assessment page of the digital continuity website nationalarchives.gov.uk/information-management/our-services/dc-risk-opportunities.htm

To help you to manage change, guidance is available from the National Archives amongst our 'Stage 4' guidance.[14] This includes managing digital continuity through MoG change, guidance on digital continuity for change managers, and advice on migrating information between EDRMS systems.

6.6 Supporting services

To support your development and implementation of an IAR, there is a framework of services and solutions held at Buying Solutions. The framework covers a variety of areas of digital continuity management, including IARs. Suppliers have been specifically chosen for their ability to:

- undertake enterprise-wide audits of information to determine factors such as format, volume, usage and location
- develop and implement retention schedules for information
- deliver efficiencies and increase value for money by analysing business processes dependent on information and implementing new information management systems, policies or procedures
- develop and implement information architecture based on file plans, vocabularies, taxonomies, ontologies or metadata schemas
- undertake information risk assessments, including assessment of compliance with legislative and regulatory requirements and other information or records management standards as appropriate.

This framework is now available. See the Buying Solutions website for more details www.buyingsolutions.gov.uk/

[14] Stage 4 guidance nationalarchives.gov.uk/information-management/our-services/digital-continuity-stage-4.htm

Appendix – Scenarios

Some scenarios and examples of IARs and processes based on the objectives set:

Managing risks and improving governance; managing retention and disposal

A small government organisation has business information stored across a number of shared drives, stand-alone databases, and an Electronic Document and Records Management System (EDRMS). Current data protection risks are not well managed, partly because of a corporate lack of understanding about where information is and how long it has been there. At the same time the organisation is looking to reduce its IM and IT costs by getting rid of information it doesn't need.

The organisation decides it should initially map all of its information assets at a high level. Each department is asked to describe on a spreadsheet the different types of information it creates and uses. The decision about how to describe each type of information is devolved to departments to ensure descriptions are relevant and useful at the business level. Departments are also asked to say how long they need to keep each information type for business, legal or archival purposes, whether there are sensitivity issues with any type, where the information is stored, whether the information type is a key corporate asset, whether any information type is no longer needed for any purpose, and the size of the data.

Completed spreadsheets look like this:

Information type	How long to keep	Sensitivity	Where stored	Key corporate asset	Can be destroyed now	Data size
Strategic planning	Long term	FOIA exemptions	EDRMS	Yes	No	Small
Public complaints	Medium term	DPA	Standalone database	No	No	Small
Building plans	Long term	No	Paper files	Yes	No	Small
Project X	Short term	No	Shared drive A	No	No	Small
Weblog files	Short term	DPA	Server Z	No	Yes	Large

The information management (IM) team collates every spreadsheet into a single workbook. This forms the nucleus of the organisation's Information Asset Register. The IM team are then able to:

- identify information types which need protection, e.g. personal data, and to review whether the arrangements are adequate
- identify with the IT team which information/data can be immediately destroyed
- allocate retention schedules to the information types
- analyse the location patterns of information and decide, for instance, whether some information types should be transferred from shared drives to the EDRMS
- identify key corporate information assets and assess whether these are being exploited sufficiently.

Working with the IA team, the IM team also ensure that the information assets described in the workbook are mapped properly to the organisation's Information Asset Owners (IAOs), and identify and fill any gaps.

The act of describing information assets in this way has allowed the organisation to better identify and manage its information risks and opportunities, and improve information management and governance. It has also resulted in cost savings through the destruction of data that the organisation no longer requires.

Subsequent to this exercise, the IT and IM teams have decided to expand the IAR to include fields about technical issues, e.g. suitability of systems for the information type, and file format obsolescence, and technical and business change issues which might impact information, to ensure digital continuity can be addressed going forward.

Managing change

An organisation uses an EDRMS to store and access all their digital files. The organisation has decided to migrate to a new system for a number of business reasons including cost and license terms. The information stored within the system covers everything from financial data with access restrictions and legal requirements for storage, through to trivial documents which have no further use to the organisation.

As a first step, the change managers perform a high-level audit of the information within the system, grouping the information into manageable assets defined by the different business divisions within the organisation. Each asset is assigned an Information Asset Owner (IAO)

in that business division who is then given the responsibility of filling out a form to establish the usability required by that asset.

The IAOs are encouraged to take this opportunity to review the information they have stored, deleting files which are no longer of use, tidying filing structures and improving the metadata associated with each file.

Once the IAOs have completed their forms, the change managers can compile the information into a centralised list of the assets and their requirements. They can then use this list to make sure the requirements are met by the new system and that the assets can be transferred without losing any information. Test plans can be written based on the list to assure that everything has been transferred successfully.

If this kind of change was undertaken without a thorough audit first, no one would fully understand what functionality was required from the new system, which could lead to too little, or even too much, expensive functionality in the system. Technology changes are a key threat to digital continuity, as it is very easy to lose necessary usability of assets during transfer.