The National Archives

Embedding Digital Continuity in Information Management

This guidance relates to:
Stage 1: Plan for action
Stage 2: Define your digital continuity requirements
Stage 3: Assess and address 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.

Contents

1 Introduction

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

Information is vital to an organisation. It is what we create and use to support the work we do every day to enable our organisation to perform its functions and deliver its services. Whether information is contained within email, office documents, images or datasets – to name but a few – we need to be able to use our information as required. Many organisations don't understand the complexities of how digital information works, or that the consequences of losing digital continuity can be as serious as any information loss.

Understanding how we 'use' digital information means understanding the stages or actions we need to complete when interacting with it. You need to:

- find your information – not only knowing what to look for but where, and to have the tools and skills to facilitate this
- open it – have the correct permissions and technology to make the information available
- work with it – understand what it is we need to do with our information – share it, edit it, run reports against it, update it, and have the technology in place to enable this
- understand it – so that you know what it is about, including who created it and what relationships it may have to other information
- trust it – know that the information is what it says it is, and have the confidence that it has not been altered

1.1 Managing information

We need to manage our information carefully over time and through change to maintain the usability we need. Doing so can help to ensure we operate accountably, legally, effectively and efficiently. It can help us protect the organisation's reputation, make informed decisions, avoid and reduce costs, and deliver better public services.

Digital information requires active intervention from the point of creation throughout its lifecycle to ensure it does not lose continuity. The risks arise from poor management, lack of understanding of how information supports the organisation, lack of an effective supporting technology environment, as well as changes in the organisation, management processes or technology. Good digital information management provides good mitigation against the risk of loss of digital continuity.

Digital continuity is particularly at risk during times of change. By understanding and managing your information well during times of stability, you will be better equipped to react to change – be it changes to

the way your business needs to use its information, changes to the technology that supports the information, or changes to the way the information is managed itself. If you do not properly manage these changes, you can lose digital continuity. Our change management guidance gives more specific advice on how to manage these changes.

1.2 Who is this guidance for?

This guidance is aimed at those who manage information; in other words, those responsible for ensuring the capture, organisation and retrieval of our information. In today's diverse and divided digital landscape this may be covered by many roles. For example: traditional 'information managers' tend to look after 'office' type information; website managers look after websites; business or system owners often look after data collections.

Information governance, risk management, information security, assurance and technology specialists may also find this guidance useful in understanding how their role supports good information management and vice versa. These roles may include: Information Asset Owners (IAO), information assurance or information risk managers, business, system or process owners and even Chief Executive Officer (CEO).

You should already understand what we mean by digital continuity and the key principles involved in managing it. You should also be aware that as a manager of information you have a responsibility to manage the continuity of that information. See more on the responsibilities that your organisation may need to cover in *Managing Digital Continuity*.

1.3 What is the purpose of this guidance?

This guidance will explain how you can maintain digital continuity through good management of information, hopefully using existing information management processes. It will enable you to:

- understand how information managers support the management of digital continuity
- understand what actions to take to manage digital continuity
- ensure these actions are proportionate and supported
- ensure you understand your information and its value
- ensure your information's digital continuity is managed and protected through changes in your organisation and technology
- ensure information and information management processes are continually reassessed

You may use this guidance to build or support a wider organisational digital continuity action plan, or to help assess the current information management capabilities of your organisation.

This forms part of a suite of guidance that The National Archives has delivered as part of a digital continuity service for government, in consultation with central government departments.

This piece of guidance provides you with practical information and support to help you complete Stage 4 of the four-stage process of managing digital continuity, which is to maintain your continuity. For further guidance on the strategic management of digital continuity across an organisation, read *Managing Digital Continuity*.

This guidance follows four key aspects to embedding digital continuity within the management of your information:

- Building a framework of governance (section 2) – ensuring that any action taken is supported by good policies and with the backing of senior management
- Understanding your information (section 3) – building a picture of what information is held so that all actions taken are both appropriate and proportionate to the organisation's requirements for that information
- Establishing the outcomes for managing digital continuity (section 4) – understanding why you need to ensure information needs to be **found**, **opened**, **worked with**, **understood** and **trusted** and what actions can be taken to ensure this
- Managing your digital continuity requirements through change (section 5) – ensuring that maintaining the continuity of your information is supported through any change process

Each section explains why it forms an essential part of managing the digital continuity of your information and lists the actions you should consider, how you might consider implementing them and who else you may need to work with to ensure you meet the required outcomes.

2 Building a framework of governance

Any actions you take to manage digital continuity should be done so with senior level support. Therefore, your first actions should be to establish this support. Senior managers need to recognise the risks of digital continuity loss to an organisation so that they can support and resource actions to mitigate that risk.

It is best practice to task this work to a Senior Responsible Owner (SRO) for digital continuity. So your first steps will be to find out whether such a role exists within your organisation. Your CEO, Head of Information Management or Head of Information Technology (IT) should know whether there is already a corporate approach in place to managing digital continuity.

It is important to ensure that the management of digital continuity is consistent across the organisation and that you're not acting in isolation. It is essential that the management of digital continuity becomes part of business-as-usual across the organisation, with actions firmly embedded within organisational policies and processes, and understood to be an essential and integrated aspect of providing good information management.

If there is no central management, then this guidance will at least help you begin to manage the continuity of your information, and indicate who else you need to talk to. However, you should still push for a corporate approach to be taken to the management of digital continuity. Raise the issues with your senior managers, explain the risks to losing continuity and direct them to supporting guidance from The National Archives.

2.1 What to do

The following sections list the steps you should now consider to support any actions you later take. Some of the specific details you might need will only be available once you have understood the information you are responsible for (as defined in section 3), so take a high-level approach until you have the full understanding you require.

2.1.1 Raise awareness at senior levels

Successful action requires the support and buy-in of senior staff to ensure it is both appropriately resourced and driven forwards, especially if funding is required. To do this, you will need to find out if there is an SRO for cross-organisational management of digital continuity and work with them to build your requirements into a wider strategy.

If there is no such role, then talk to your own senior managers, using supporting guidance from The National Archives to help make the case for action. Encourage them to advocate upwards through the organisation as well.

2.1.2 Establish scope and priorities for digital continuity

You need to be very clear about why you are managing digital continuity, what your reasons are for starting the investigation and what you hope to achieve from it. Considering your drivers will help you to define your priorities and starting point. These different drivers will give you different objectives, and will therefore direct the scale and scope of your investigation.

This guidance will enable you to understand and detail your continuity requirements and the teams you will need to work with to deliver them. Work with them to list all the actions that need to be taken and set milestones for the completion of each one. Managing digital continuity is an ongoing process and you should regularly review your requirements and actions.

2.1.3 Ensure you define your digital continuity requirements within your policies

Defining your requirements within the appropriate policies ensures they become part of the corporate management process. You should detail why it is essential to manage digital continuity, what you mean by digital continuity (find, open, work with, understand, trust), and the major steps you will take to support each of these.

You should consider that your digital continuity requirements are detailed appropriately within each of the following documents:

- knowledge and information management strategy
- knowledge and information management policies on the capture and organisation of information
- knowledge and information management policies on the use of metadata and metadata schemas
- retention schedule
- knowledge and information risk management strategy, policy and processes
- organisational and information management access control policies and procedures
- organisational change and project management policies and procedures

2.1.4 Ensure you document the risks to loss of digital continuity

Loss of digital continuity is a key information risk and needs to be acknowledged within all relevant risk registers so that it can be reported on and actioned when necessary.

If you do not have responsibility for updating your departmental risk register, you should work with whoever does to update it accordingly. Build an understanding of how risks are managed within your organisation, who

manages them and how they are reported. This will ensure that risks to digital continuity arising from the management of information are dealt with appropriately.

2.1.5 Ensure that your change management procedures test for digital continuity

Loss of digital continuity is greatest during organisational, technological or informational change. Any change management plan you are responsible for should ensure that digital continuity is managed through that change. Any change management plan that affects the information you manage should equally ensure that continuity is maintained through the process.

Further guidance is available to support the management of digital continuity through change.

2.1.6 Align your actions with others within your organisation

The ways in which digital information is created, processed, managed and handled can be supported across many elements of an organisation. To fully maintain digital continuity across an organisation requires all these elements to work together. For example:

- your IT team will provide the supporting technologies and systems that capture, manage and deliver your information
- your information assurance teams are responsible for ensuring information is protected but can also be exploited
- change management teams will be responsible for the way information is managed through periods of change
- the information's business owners understand how the information supports the business, how it should be used and what value it brings to the business
- IAOs are responsible for specific assets
- systems users are consulted

You need to talk to each of these teams as you start to plan your own requirements to manage digital continuity. Ensure they understand your intention and know how to support you. Equally you will need to know whether other action is being taken and how you can support that. Communication and support across the business, in areas where teams traditionally do not talk to or support one another is a major benefit to the organisation and its ability to operate efficiently.

2.1.7 Define the roles and responsibilities for managing digital continuity

Management of digital continuity needs to be made explicit within everyone's responsibilities. Staff across the organisation need to understand why they have to manage the information they create and handle in a certain way, so that they take the appropriate actions. Add a statement of responsibility to your policies for

staff to manage continuity (or issue one separately). You could update job responsibilities and specifications by adding to staff personal objectives.

2.1.8 Ensure suitable training is available for all staff that need it

All staff should be trained in the basic requirements for managing their information. This training needs to be focussed on how good practice will support staff in their work (i.e. so they can see 'what's in it for me'), be delivered in a language they understand and be topped up at regular intervals.

If you don't already have an information management training course, then build one, and ensure it becomes a mandatory aspect of new starter training. Ensure top up sessions are available for all staff every year to two years. You could also add 'how-to' and 'best-practice' guides for good information management in a clearly defined section of your intranet.

Digital continuity training is offered by The National Archives. There may also be useful courses available on the Civil Service learning platform.

3 Understanding your information

Being able to use your information means being able to find, open, work with, understand and trust it. Of course, these requirements will vary between different types of information and over time. For example, to work with an active document you may require the ability to edit that document, whereas if that document is selected as an archival record for transfer to The National Archives then it will need to be held in a state where it cannot be changed in order to reflect the nature of the document when it was selected.

However, even before you can determine your usability requirements, you need to know what you have, where it is, and what functions that information supports.

3.1 What to do

The following sections list the actions you should consider taking in order to understand your information. If you have not already done so, this process will build a picture of what information you are managing, which can then be documented and used to support further decision making.

Again, before you start, think about how you are going to do this and how it fits with similar work being carried out across the organisation. Are you working independently across the information you are responsible for managing or are you undertaking this kind of assessment as part of a more complete plan to build (in small, manageable stages) a complete picture of the organisation's information? Ultimately you want to align all actions taken within a wider organisational plan for managing digital continuity.

You also need to think about how the values you assign may change over time and capture these. For example, sensitive or protectively marked information may only remain so for a specific period of time. Highlight additional risks to the information as you classify it.

3.1.1 Define the level at which you are going to analyse the information

With hundreds of thousands, if not millions of objects being held, you need to make your analysis at a proportionate, and therefore useful, level.

Apply standard information types, either specified by The National Archives or already in use within the organisation (for the creation of metadata fields, or retention schedules). You may also want to have specific values set against different business units, projects or programmes.

3.1.2 Identify information owners

Information owners will understand the business requirements for the information their teams create and can support your understanding of it.

You can start by approaching each business, project or programme owner, or heads of department directly. Additionally, if your organisation manages an *Information Asset Register* (IAR), talk to the register owner to identify each individual asset owner.

3.1.3 Identify where the information is

Information can be held across multiple systems or in numerous locations that you need to understand so you have the appropriate technology in place to support them. Furthermore, information held on external media or on bespoke systems is subject to further risk (see section 4.1.2) and can often fall outside of corporate management processes.

First, you need to identify whether you are managing a single or multiple assets and who the main business owners are of the systems they cover. Information owners should know what information sits on the systems they are responsible for. However, a discussion with business, project or programme managers may reveal additional information stores, or use of external storage. Your IT department should hold a list of all systems in place.

3.1.4 Define retention requirements

Information shouldn't be kept longer than is needed to fulfil its purpose. Information held unnecessarily is still at risk and subject to legal requirements such as Freedom of Information (FOI) or Data Protection Act (DPA). If you don't already have retention schedules in place, working out the following generic requirements can help you build them:

- transitory information
- information subject to particular legal retention periods
- information to support the organisation's functions in the short, medium or long term
- information required for inquiry
- information required for the archival record

3.1.5 Identify any specific risk associated with the information

This includes:

- reputational risk
- inability to perform functions or services
- cost of recovery
- sensitivity such as personal data or protectively marked information
- whether information is password protected or encrypted

- whether the information needs to be made available outside the organisation, perhaps to related bodies or agencies (or is even being held on their behalf), or to the public through the web meeting transparency agendas

Certain types of information hold specific risks associated with them and therefore need to be managed differently from others.

Talk to the business, project or programme managers who create or work with the information to agree on levels of risk. If the information falls within identified information assets then talk to the IAOs. You should also talk to information risk managers, who will have a good overall view.

3.1.6 Identify how old the information is

As information gets older there is an increased risk that you won't be able to open or work with it. This could be due to hardware or software obsolescence, decay, or older information not being managed as well when requirements for doing so were less certain (e.g. they may not contain the required context to enable understanding or trust).

You can use The National Archives' DROID tool which can be run across file stores and will deliver reports on the age of the information you hold. Systems holding the information may also be able to provide you with data on the ages of files.

3.1.7 Identify what file formats they are held in

You may need specialised technology to use older or bespoke formats. An understanding of what formats are in use may also help your IT rationalise what applications are required, allowing them to migrate information to more efficient systems.

As above, you can use The National Archives' DROID tool which can be run across file stores and will deliver reports on the formats of the information you hold.

We have also produced guidance on DROID which will help you to evaluate your file formats from a digital continuity perspective and employ strategies to maintain the continuity of your digital information.

3.1.8 Document your findings

You should document all of the data you have collected so that it can be shared or re-used within the organisation, used to support action, and re-assessed on a regular basis.

The most suitable location to document your findings are in an expanded IAR – by which we mean an IAR that covers all information assets and not just sensitive or personal data. Overall responsibility for an

organisation's IAR is most likely to be held by its information assurance team. Talk with the team to determine how you can support the wider risk management of your information through using an IAR. You can support your arguments referring to the information asset guidance from The National Archives.

If your organisation does not have an existing IAR, you can use the template provided by The National Archives to build an IAR for your own information assets and document your findings.

4 Outcomes for managing the digital continuity of your information

The outcomes from managing digital continuity are that your information can be found, opened, worked with, understood and trusted. This section explores the actions you can take to ensure this.

It is worth repeating here that the extent to which you meet each outcome will depend on the nature of the information itself – this will already have been determined following the previous section. The specific requirements for delivering each of these outcomes against all your information types form your digital continuity requirement and should be stated within your information management policy.

4.1 Ensure you can find your information

Information must be findable by those who need it. This means keeping information in a logical place, ensuring staff know where to look and how to look, ensuring it can be found using your search technologies, while also ensuring that those who should not be able to find it, are unable to find it.

4.1.1 Understand the requirements for your information to be found

You need to know whether there are any specific requirements, for example, if you're likely to have FOI requests for some types of information and whether they can be managed appropriately.

Use the details you have documented in your work understanding your information to define your specific requirements for finding information. Where you have identified risks, ensure that mitigation solutions can be, and are, put in place. You should consider:

- how much of the organisation needs to access your information
- whether or not it is covered by corporate search tools
- any specific requirements for discovery (FOI, inquiry, etc.)
- any specific risks associated with the information type, for example email. If it is held on email servers, how easy will it will be to find email across the organisation if it is not stored elsewhere? Email may also hold relevant attachments. Specific requirements for email should be held within an organisational strategy for email management
- any specific risk to the information being found by staff who shouldn't have access to it
- any specific risks to information that can't be held within the standard corporate locations (such as information types that cannot be held due to the complexity or size of the formats), or where specific types of information (for example, datasets or websites) are held in specific storage locations

4.1.2 Ensure information is being captured in the right locations

Information should only be held in managed locations. Information not held in a well-managed location is at increased risk.

You must inform staff of where they should be capturing business information and encourage the appropriate use of shared or personal drives – if necessary limit access to these spaces. Do not allow long-term exemptions and revisit any exemptions granted on a regular basis. You should also limit the use of external storage media wherever possible and ensure you have a management strategy in place for the use and maintenance of external media, including regular testing.

You should encourage staff to move business information to such areas, ensuring the continuity of that information is managed through the process. If information cannot be moved, ensure these locations can be easily accessed and that a list of the locations and the information they hold is made available to all staff. Where external media is required to hold information, or where transfer cannot be managed, ensure the media is managed in a central location with the content types indexed.

4.1.3 Ensure organisational filing structures enable discovery

The context provided by organisational filing structures also supports browsing through those structures. If they are not easily understood, they may prevent staff from finding the right areas they are looking for.

For document filing structures across drives or document management systems, you should undertake an analysis of the organisational structures you use, working with business units, and project or programme teams as appropriate. Make changes as required.

For information hosted online, undergo usability and user-interface testing. For all other information delivery or storage locations, you should ensure the organisation of that information supports hierarchical browsing in a meaningful way, according to user need.

4.1.4 Ensure metadata supports your search

Search tools run across indexed metadata fields to provide search results. You need to ensure that the metadata fields you capture can be searched, and also that they support the search behaviours of your staff.

First, you'll need to talk to IT to understand how your corporate search tools work and what they search against. Next you should undertake an analysis of search behaviours within your organisation. Use a small sample of staff from across the organisation and examine how they go about finding information. You should include staff responsible for searching for information on a regular basis such as FOI teams and work with IT to make changes as required.

4.1.5 Ensure information can be indexed for search

Certain formats (for example, some older types of PDF) cannot be indexed for searching, preventing discovery of the information. You'll need to work with your IT team to identify the formats you manage that cannot be indexed.

4.1.6 Support the efficiency of your search tools

Tools need to be user-friendly and fit for purpose to support effective and efficient working.

Undertake an analysis of your search tools, document the results and make suggestions as to what's required to improve their efficiency, whether it is a replacement tool or an opportunity to reconfigure existing technology. You'll need to understand what staff search for and how, and assess the ability of the tool to return both comprehensive and useful results.

Draw up a testing regime alongside your IT team, who should understand the technology requirements for the search tools. When testing the scope, include teams who regularly search for information (such as FOI teams).

You may also want to consider the use of e-discovery tools within your organisation (i.e. if your search requirements not met by current tools available) and how you are able to respond to e-discovery requests if they come in. E-discovery tools will provide specialised search facilities, but may be considered too costly to act as a corporate search tool.

4.1.7 Ensure staff know how to search

Searching is a skill, and staff may not have advanced search skills. You need to ensure you fully understand how your search tools work so you can develop a suitable training programme. You can then implement training workshops and make 'how-to' guides available to all staff.

4.1.8 Ensure metadata is entered correctly

Incomplete or inadequate metadata entries will mean you cannot find your information, as it will not appear in search results or against search terms.

Ensuring you apply user-friendly standards to metadata entry is the only way to achieve a level of standardisation that will promote the easy finding of information. Automated metadata entry may be possible for some fields.

If vital metadata is missing or suffers from data quality problems, it might be appropriate to use tools to rebuild and improve it.

4.1.9 Dispose of unnecessary information

Holding more information than you require may slow down search tools or deliver too many unnecessary results. Ensure you have agreed retention schedules in place and that information is being disposed of accordingly.

4.2 Ensure you can open your information

You need both the appropriate technology and access permissions to be able to open digital information. Your IT department or external supplier will provide your technologies, however it is important you understand what applications you need to deliver the information you manage. It is important that you document this, and a comprehensive IAR may be a suitable place to do this. IT may also retain similar information within a Configuration Management Database.

It is worth remembering that when new information is transferred into the organisation new formats may be introduced that your organisation does not use so you must have applications in place to support the, if they are required for business use.

4.2.1 Understand your requirements for information to be opened

You need to be able to ensure that the right staff are able to open the right information and that you are able to facilitate this by understanding what is required and that this is documented, preferably within a comprehensive IAR.

Ensure that you at least have a documented list of which information requires particular access permissions in place, and which information is password protected or encrypted. It is also useful to know which applications are required to support the information formats you manage and to work with your IT team to ensure the technology is in place to open them.

4.2.2 Maintain the correct access permissions

Information should only be available to those who need it. If unmanaged, access permissions can prevent staff from accessing information they should be able to access, or allow them to access information they shouldn't.

Access permissions tend to be set against a specific user, recognised through their account login and administered by HR or IT, possibly alongside the organisation's security managers. You may, therefore, simply want to ensure they are being administered suitably by requesting details of how they are granted and updated. Access permissions should at least be revisited when staff join, move within, and then leave the organisation.

You may be able to set permissions within the systems you manage in which case you need to understand how to set permissions and define where access controls need to be set. This is usually easiest when applied at a suitable organisational level. Set permissions against groups to which single users can be added or removed, not against a specific individual.

4.2.3 Maintain knowledge of password protected information

Passwords can be set to prevent access to entire systems (often databases) or specific pieces or groups of information. You can lose the ability to access this information if those who set the passwords move on without ensuring ownership of the password is also passed on, or if knowledge of what is password protected is lost.

You won't be able to maintain a list of passwords themselves, but you can maintain a list of password protected information and their owners that can be maintained. You need to ensure there is a process in place to tell you when a password owner is changing status within the organisation and can manage a re-set or handover of the password as appropriate. This information would usefully be maintained within a comprehensive IAR.

4.2.4 Maintain encryption keys

Encrypting information is another process to ensure it cannot be read or accessed. If knowledge that information is encrypted or the encryption keys themselves are lost, access to the information will be lost, and potentially very expensive to recover.

Encryption will most likely be managed by your IT team working alongside your security or information assurance specialists. You should ensure you are aware of whether you are responsible for managing encrypted information, who manages the encryption keys and what procedures are in place to do so. This information would also usefully be maintained within an IAR.

4.3 Ensure you can work with your information

Being able to work with your information can mean anything from reading a text document, to querying a dataset. Your ability to do this is entirely dependent on the supporting applications, again usually provided by your IT department or supplier. However, you are best placed to determine how certain types of information will need to be used and whether that use will change over time, and therefore express their requirements for the technology solutions that will need to be delivered. You might do this against the format or the type of information. You should document this individually and, if possible, within an IAR.

4.3.1 Define how you need to work with your information

It is important you define how you need to work with your information so that the appropriate technology support can be provided. You can use your previous investigation of information types (within your retention schedules, see section 3.1.4) to work out the usability requirements.

Work out your organisation's generic requirements for working with information and apply them to each information type. These requirements should be developed alongside each business unit and owned centrally and may include:

- read (and variations of: watch, listen, etc.)
- edit or change or update
- publish or share (internally or externally)
- query or analyse or report against

Then assess whether the 'work' requirements will change at all. In some cases, business information required for long term support, or the archival or historical record may need to be locked down so that they cannot be changed.

These requirements need to be documented, both within your information management policy, but if possible, also against your IAR.

4.3.2 Ensure that appropriate supporting technology is in place

Some technology may enable you to open and read information, but not edit it. This can work against certain older formats and updated versions of their supported application or bespoke applications used to support other proprietary formats. You can support the delivery of the right technology by ensuring you are supporting your procurement and IT teams with the appropriate requirements.

Analyse your information for older formats using the DROID file profiling tool from The National Archives and alert your IT team for old or unfamiliar formats to ensure they can be opened using available technology.

Ensure that when new information is transferred into the organisation, the requirements to work with that information are understood and that new supporting technology is in place if required. Make your IT team aware of these usability requirements to determine whether information can be moved or migrated to more cost-effective or efficient systems or formats.

4.4 Ensure you can understand your information

Understanding your information is as much about knowing where it is from and what it relates to as it is about knowing what it is. The way in which we describe our information comes from both the way in which we organise it and the metadata we attach to it.

4.4.1 Organise your information appropriately

The way in which you organise your information enables staff to understand what parts of the business it relates to, which team created it, and even what type of information it is.

You should:

- gather requirements from your business units, if you are building a new structure or file plan
- put limits on the number of layers that can be added and ensure that adding to the file plan is well administered to avoid it becoming too large and out of control
- if possible, capture metadata about each level of the structure within the hierarchy, usually possible with document or records management systems
- ensure that you apply useful naming conventions to describe levels within a hierarchy
- ensure staff understand their responsibilities so that they also capture information within the right areas of the hierarchy
- ensure datasets are usefully named

4.4.2 Use appropriate metadata

The metadata that describes information needs to do so simply and clearly, and be applied in a complete and standard manner across all your information. Metadata will vary between types of information (for example, documents or photographs) and you will need to capture the right metadata for each information type.

Most importantly, you need to define your requirements for the minimum metadata you need for each information type you are managing; you may already have set organisational standards for this.

Ensure your policies and process support the correct completion of metadata, and that staff find it easy to do so and understand why they have to do so – staff will rarely enter additional metadata willingly.

If possible, use automated metadata capture or completion. Limit choices through the use of drop down menus if possible. If you have not undertaken an exercise to assess how your information systems capture metadata, then you may wish to do so and make recommendations for change based upon this.

4.4.3 Manage and maintain relationships between and within information

You can acquire understanding about information through its relationships with other information, such as: parts of a series, virtual reference links to other information in a system, or attachments to an email. If these links are broken, you may lose understanding.

Define your understanding of the way information is linked within your systems and ensure that you have a policy in place that determines why those links need to be maintained. You'll then need to work with your IT team to ensure that processes are in place, especially through a moment of change, to maintain those links.

4.5 Ensure you can trust information

Trusting information means you are confident it is what it says it is. You are confident it is genuine, are aware of any changes that have happened to it, and confident it has not been maliciously or accidentally corrupted. This is very much related to the notion of integrity used in information assurance and your work here should be undertaken alongside your IA specialists.

4.5.1 Manage version control

If multiple versions of a single piece of information exist, then you need to know which of them is the most recent, especially if each previous draft or iteration forms an important record in themselves.

Some document management systems will automatically capture versioning when a single document is changed. In all other cases, you should have a standard format for versions applied across the organisation and ensure all staff are aware of how to use it and do so.

4.5.2 Know when information is changed or moved between systems and who moved it

If information is lost or changed, either unintentionally or maliciously, then it can be questioned or may prevent services from being delivered. You will have to rely on the logs kept by your information systems as to who moved the information, where to and when. The logs will be held by your IT team and your information assurance specialists and IAOs will also want to have access to this data.

Most systems should maintain audit trails of movement within and outside that system. You should talk to your IT team who can tell you how this is captured and how long it is held for. You may feel that it is important to capture audit trails for sensitive or personal data for longer periods than other types of business information. You will need to think about the digital continuity of any logging or audit data you need to retain for long periods.

5 Managing change

Loss of digital continuity is greatest at times of change; whether this is change to the business, the technology or the information itself. Change may force you to reassess your continuity requirements and establish new ones, or ensure that an existing state of continuity is maintained through that change.

The requirements for how information needs to be managed through change should form an essential part of any change project that could affect that information. Without these requirements, continuity can easily be lost.

More complete guidance on managing digital continuity through change is available from The National Archives. It is essential that information managers define the requirements for the continuity of information, impact assessments for how information may be affected by change and test plans to ensure that continuity is managed through change.

If information management requirements are not currently included within change management processes, or not being defined by the right people, then you need to ensure that you escalate the need and reasons for doing so to senior management.

5.1 Ensure your requirements form part of change management planning

Your continuity requirements will determine the level of completeness and availability that have to be maintained, affecting the management of both the information and the systems it is held on through the change. Without them, the change management planning may well allow for continuity risks to creep in.

Use the continuity requirements you should already have defined. Think about the need to maintain:

- your usability requirements – the need to find, open, work with, understand and trust your information
- the structures by which information is organised
- requirements for the metadata and the quality of that metadata to be maintained
- logs or audit trails that need to be maintained
- relationships or links to other information that need to be maintained
- access restrictions
- information about sensitivity such as protective markings

5.2 Develop an impact assessment

Any assessment of the need for change must include the impact of that change upon the organisation. The impact of change upon the usability requirements or the ability to maintain them needs to be included so that you can assess risks to loss of continuity.

It is best to work with your change management teams to build an impact assessment for information, or talk to other organisations that may already have them.

5.3 Develop test criteria

Without testing after change against a set of specific measurable criteria, you will be unable to assess whether continuity has been maintained.

Work with your change management team to build a suitable test programme, using your understanding of the continuity requirements. Choose appropriate selections of information to test against, reflecting the diversity of information held across the organisation.

6 Next steps

When you manage your information well and it is supported by the appropriate technology environment, your organisation can be confident it is able to provide the completeness and availability required to deliver the usability the organisation needs from its information.

This guidance has listed the key factors an organisation should have considered and embedded within its information management policies. You can now use our checklist in the Appendix below to ensure you are aware of all the principle issues involved in maintaining digital continuity and that your policies and processes are meeting the business's need to manage digital continuity.

If you identify issues that are not being managed, you should be escalate these to your digital continuity SRO, if there is one, or the CEO or Executive Team, to ensure that resources are made available if necessary. However, in the long term, all actions that manage digital continuity should be part of business-as-usual and embedded in your existing information management policies and procedures.

Appendix: checklist

Building a framework of governance

- ☐ You understand the information you have and the value it has for the business
- ☐ You have made information management staff aware of their roles and responsibilities for managing digital continuity
- ☐ You have identified and engaged others across the organisation involved in the governance of information and have a mutually supportive relationship
- ☐ You have embedded digital continuity into existing IM strategies and policies, and have added risks to digital continuity into existing risk registers
- ☐ You have ensured your requirements for how information is to be maintained through change are delivered to the teams managing that change
- ☐ You have developed an impact assessment and test criteria to ensure change is successfully managed
- ☐ You re-assess your actions every one to three years to ensure they still deliver on your requirements and meet business needs
- ☐ You take regular snapshots to confirm procedures are being followed and report back on any failings

Outcomes for managing information

Ensure you can find information

- ☐ You have defined appropriate locations where information should be stored
- ☐ You have restricted access to other possible locations for storage
- ☐ You have moved orphaned or unmanaged information into managed locations
- ☐ You have retained accurate metadata
- ☐ You have ensured your information can be indexed
- ☐ You have ensured your staff know to search accurately
- ☐ You have disposed of any unnecessary information
- ☐ You have managed access restrictions

Ensure you can open your information

- ☐ You understand the applications you need to deliver the information you manage, and are able to work with IT to ensure the appropriate technologies are in place
- ☐ You have maintained encryption keys
- ☐ You have maintained passwords and access permissions

Ensure you can work with your information

- ☐ You have determined how certain types of information will need to be used over time, for instance, requirements to read, edit, share, publish or protect the information
- ☐ You have recommendmmed to your IT department or supplier what technologies are required to use the information in these ways

Ensure you can understand your information

- ☐ You have organised your information in a way that allows you to understand where it's from and what it relates to
- ☐ You have defined the appropriate metadata you need to describe and search your information
- ☐ You have maintained relationships between and within information, including email attachments, related files and hyperlinks

Ensure you can trust your information

- ☐ You are confident that your information is genuine, that it hasn't been tampered with and that you are aware of any changes to it
- ☐ You work alongside your information assurance specialists
- ☐ You document who is moving or changing information and when
- ☐ You have a policy for managing version control