The National Archives

Change Management for Digital Continuity SROs

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.

If you do not actively work to ensure digital continuity, your information can easily become unusable. Digital continuity can be put at risk by changes in your organisation, management processes or technology. You need to manage your information carefully over time and through changes to maintain the usability 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.

1.1 What is the purpose of this guidance?

This piece of guidance describes how to manage and protect your digital continuity through change, to ensure your business-critical information remains usable. It will help you understand:

- why change is such a risk to digital continuity
- the impact of different types of changes
- who you will need to work with to manage change

Finally, we propose a process you can follow during a specific change to put you in the best place to minimise the risks to your information.

This guidance 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.

We assume that you have a good understanding of both what digital continuity is, and how it applies to your organisation. Change management is part of the final step of the four-stage process for managing digital continuity – so ideally you will have completed the first three stages and therefore have identified and documented your information assets and the risks associated with them.

1.2 Who is this guidance for?

This guidance is aimed at those responsible for looking after information and its digital continuity. Primarily this is the Digital Continuity Senior Responsible Owner (SRO), who should have been appointed by the Chief

Executive Officer (CEO) or equivalent manager at board level, to manage digital continuity across the organisation. The guidance may also be helpful to Information Asset Owners (IAOs).

There is a separate piece of guidance, *Digital Continuity for Change Managers*, which explains digital continuity and the risks and issues for change and project managers. It is a 'one-stop-shop' for people who have to manage changes, starting from a description of what digital continuity is, and taking them through to the specific risks and issues associated with particular types of change.

See more on the responsibilities and related roles that your organisation will need to address to ensure the digital continuity of your information in *Managing Digital Continuity*.

2 Why does change affect digital continuity?

You can only use your information in the way you need for as long as you need when your technical environment and information management appropriately support the business use you need from your information assets (see Figure 1 below). This happens when:

- you know **what information you have**, what it is about and where it is
- you understand **how you want to use it**, now and in the future
- your **technology and information management processes enable** you to use your information, and are agile enough to cope with changing requirements

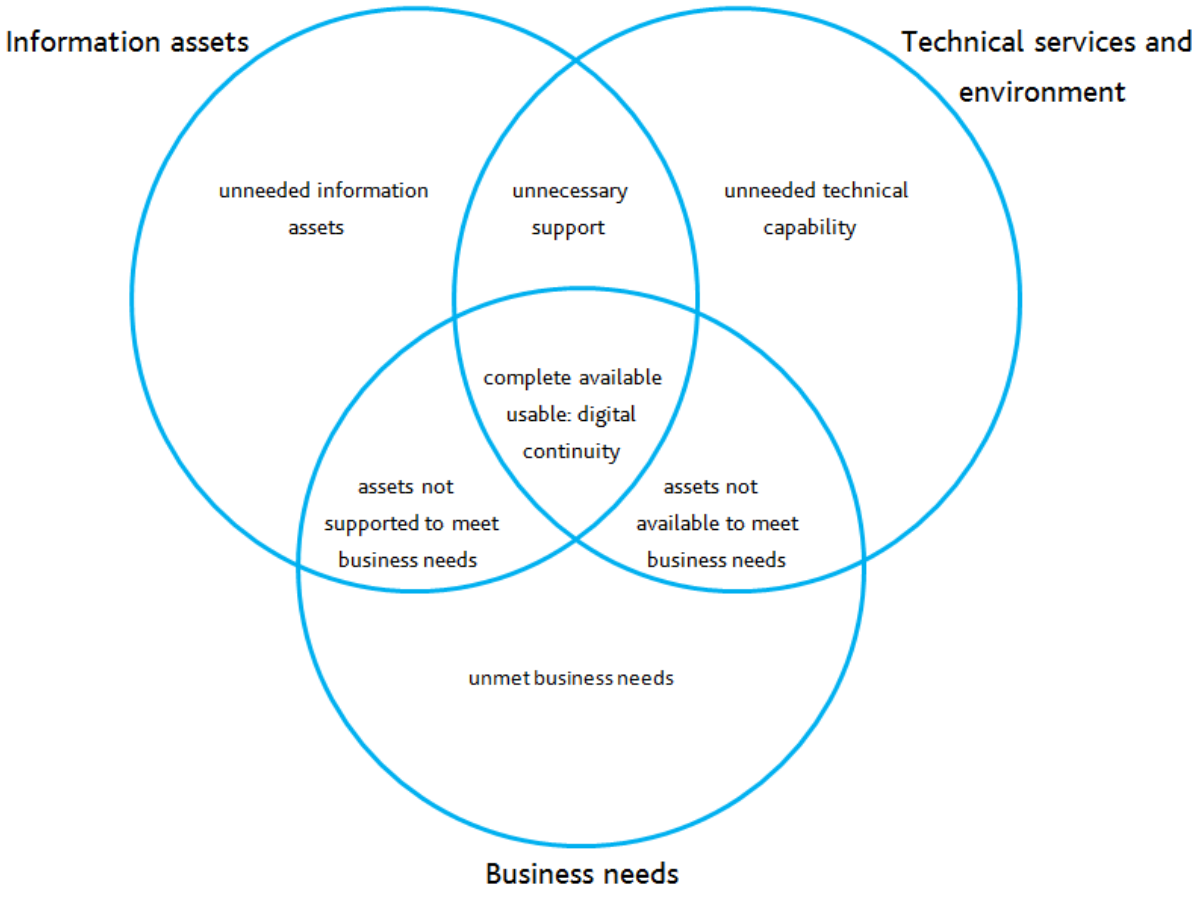

Figure 1: ensuring digital continuity

Digital continuity is about managing the complex inter-dependencies between your information assets, your business needs and your technological capability so that they remain aligned. Changes to any of these elements could break this alignment and have a dramatic impact on your ability to use your digital information.

Digital information is dependent on the technology you use to access it and the processes you have in place to structure and organise it. This makes digital information particularly sensitive to changes across your organisation – changes in technology, the way you manage information and to your business needs.

Government is experiencing widespread change to function, organisation, technology and policy and these changes increase the risk that we will lose access to valuable information, as:

- significant projects close
- organisational structures change
- agencies, Non-departmental public bodies (NDPBs) and organisations close
- staff move or leave
- IT systems are replaced, upgraded, outsourced or moved to cloud-based services

These can all have serious and long-lasting repercussions to your ability to use your digital information in the way you need, now and in the future. Even seemingly minor changes, such as a single member of staff leaving or a minor upgrade to a piece of software, can have an impact.

These types of change can raise the risk that you will lose the ability to access some or all of the information you rely on, resulting in situations where 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 is about
- **trust** your information is what you say it is

Managing change to deliver digital continuity will enable you to continue delivering services effectively, to re-use and refer back to critical information at a later date, and to provide a record of government.

2.1 What is your role?

As Digital Continuity SRO, you should act as an advocate for your organisation's information, ensuring digital continuity requirements are considered early enough in the process so that they can be smoothly incorporated into planning. It is almost always easier to maintain digital continuity through forward planning, than it is to re-establish it once it has been lost. If concerns are raised late in the project, it is much harder to address them without disruption or expense.

You must be proactive in making sure that key people in your organisation, such as project and change managers, heads of information management, IT and information assurance are aware of the risks and issues related to information assets. For smaller changes, these individuals should be able to manage these risks and issues themselves, contacting the relevant IAOs whose assets are directly impacted. They should only need to involve you in larger-scale projects which may have a more significant impact, or impacts, across multiple assets.

The process of managing change should be a dialogue – there may have to be compromises made on both sides of the process. You may accept risks to, and constraints on, your ability to use your information in some way, to realise the wider benefits driving the change. Or you may need to adjust your scope and timescales to better protect the digital continuity of business critical information. However, it's important that everyone works from an informed position, so that you have a shared awareness and acceptance of the impact upfront, rather than being surprised by problems that emerge later on.

2.2 How can you prepare for change?

The four-stage process for managing your digital continuity will equip you with the understanding that you need to better manage changes, large or small, in your organisation. By understanding your current assets, business requirements and technical environment you will be better placed to assess the impact that a specific change to any of these areas will have on your information quickly, clearly and confidently.

As part of the process you may have created or updated a number of tools and processes which can provide this understanding, such as:

- *Information Asset Register* (IAR) – documenting your assets and their usability requirements
- Technical dependencies mapping – documenting how the technical environment supports those usability requirements. This may be recorded with the IAR, a Configuration Management Database (CMDB), or a number of other types of register
- Risk assessment – documenting and analysing particular risks and issues to your information assets and digital continuity

You must keep informed of upcoming changes and the potential impact they may have on your information. This may come via the CEO or Executive Team, but will depend on the structure of your organisation.

You should liaise with change management teams either at an organisation level or a department level to make sure that digital continuity issues are covered within their change processes. Our guidance *Digital Continuity for Change Managers* explains the issues for this audience and provides advice on how they can include management of digital continuity in their existing processes.

For each type of change listed in section 3 below, you may want to consider what processes you can put in place in advance to reduce the risk of minor changes affecting your digital continuity. For example, you can work alongside your HR team to make sure that exit processes are in place, so that when staff leave any information management issues are raised and understood.

3 Type of change

As shown in Diagram 1, change factors that affect digital continuity can broadly be grouped into three categories:

- changes to the way the business needs to use its information (section 3.1)
- changes to the technology that supports the information (section 3.2)
- changes to the way the information is managed (section 3.3)

Each of these types of change is likely to be driven by different departments who may have different ways to manage change and have varying levels of understanding and consideration for information management and digital continuity. Your own responsibilities and level of involvement will vary accordingly.

The Appendix contains more examples of each type of change and their impact.

3.1 Business change

Your business requirements drive the way that you need to use information. Any change to what your business does, or how it does it, can have a corresponding effect on your information. If your business change has an impact on how you need to use your information, you will need to perform an assessment to make sure that the new requirements are fully supported by your technology environment and information management. Business change often necessitates extensive knock-on changes in other areas, so you will need to make sure that you can support your new usability requirements.

A business change may influence only one of your usability criteria – for example, a change to your security policies which requires an amendment to who can open a specific asset. Alternately, it may affect a number of different usability requirements. For example, a Machinery of Government (MoG) change involving your organisation merging, dividing or closing down altogether, may necessitate a large-scale review of your information's usability requirements.

Who is involved in business change?

Business changes may be run according to a strict process and involve project and change managers. However they may also be done in a very ad hoc manner, often not really acknowledged as a 'change' at all. A large number of systems and individuals can be affected.

3.2 Technology change

The most obvious threats to digital continuity are changes to the technical environment which supports the use of your information assets. This type of change can be gradual, in that certain technologies become dated

over time, or isolated – for instance, you may just be upgrading one piece of software. However, even such isolated changes can be made up of lots of smaller types of change – for instance, an EDRM migration may involve not only software changes, but also file format and technology management issues.

Who is involved in technology change?

Technology changes are usually managed from within the IT department, often within a small team with responsibility for the specific system which is going through the change. If the system (or even the entire IT department) is outsourced, the change will likely be managed by that company, with an internal contact.

Change management for technology changes are generally strictly mapped out from the start of the project and will often be taken from centralised processes. There are likely strict processes in place for managing the change and your organisation may have dedicated technical change and project managers.

Occasionally ad hoc technology changes are made, independent of the IT team and their processes. For example, a department may choose to introduce a new piece of technology or system without wider consultation. This might be done through external providers directly or through web services. These changes are often poorly managed and fail to follow the organisation's processes. This can lead to isolated systems and information which is at greater risk of digital continuity loss.

3.3 Information and information management changes

The very processes that look after your information can sometimes themselves change and, if you do not properly manage them, you can lose digital continuity.

The way your information is managed varies between different organisations. You may have formal written policies and processes, documents and registers to manage your information – for example, retention schedules and IARs, metadata policies and file plan structures. There may be a dedicated team to manage information, with networks and extensive support for IAOs. Whatever processes your organisation uses to manage information, any changes to those processes will have an effect on your information, and you must ensure that assets or aspects of their usability requirements don't fall through the gaps.

Knowledge and expertise in the understanding of assets and how they are used can be lost when members of staff leave or even just have extended periods of time off.

Who is involved in information management change?

You are likely to be working with people in your organisation responsible for information management – IAOs, Information Assurance (IA) and Information Management (IM) teams. It may even be that you instigated the change or are managing it yourself and that a driver for the change was to improve digital continuity.

4 Managing change

Each organisation plans and manages change differently depending on their scale, structure, available resources and risk appetites. Ideally your organisation will have a change process which is followed or adapted for each specific change and you can embed management of digital continuity into that process.

How the change is managed, your role within that process, and the input you can have in it, will vary. You may find your established change management process has digital continuity already embedded within it, or maybe you are in a position where you are able to influence the process and improve it, either at a strategic level, or for the specific change you are looking at.

However, it is not always possible to be involved with the process at this level, for example when dealing with a change managed by an outsourced IT provider. In these cases it may be better to take the actions required independently of the main change process. You need to make sure that someone is assessing the impact of the change on the information, performing a risk assessment and drawing up a list of requirements or action points which is then shared with those managing the change. They can then incorporate these actions and risks into their existing processes.

Managing Digital Continuity outlines a four-stage process enabling you to make sure you understand and protect the digital continuity of your information. You can apply this process on different scales – either to all the information an organisation holds, only to a specific sub-set of that information, or only to that information which will be affected by a specific change. This granularity allows you to address your digital continuity in manageable sections in a timely way and is particularly useful when looking at change.

The four stages of managing digital continuity are:

- Stage 1: Plan for action
- Stage 2: Define your digital continuity requirements
- Stage 3: Assess and mitigate risks to digital continuity
- Stage 4: Manage digital continuity

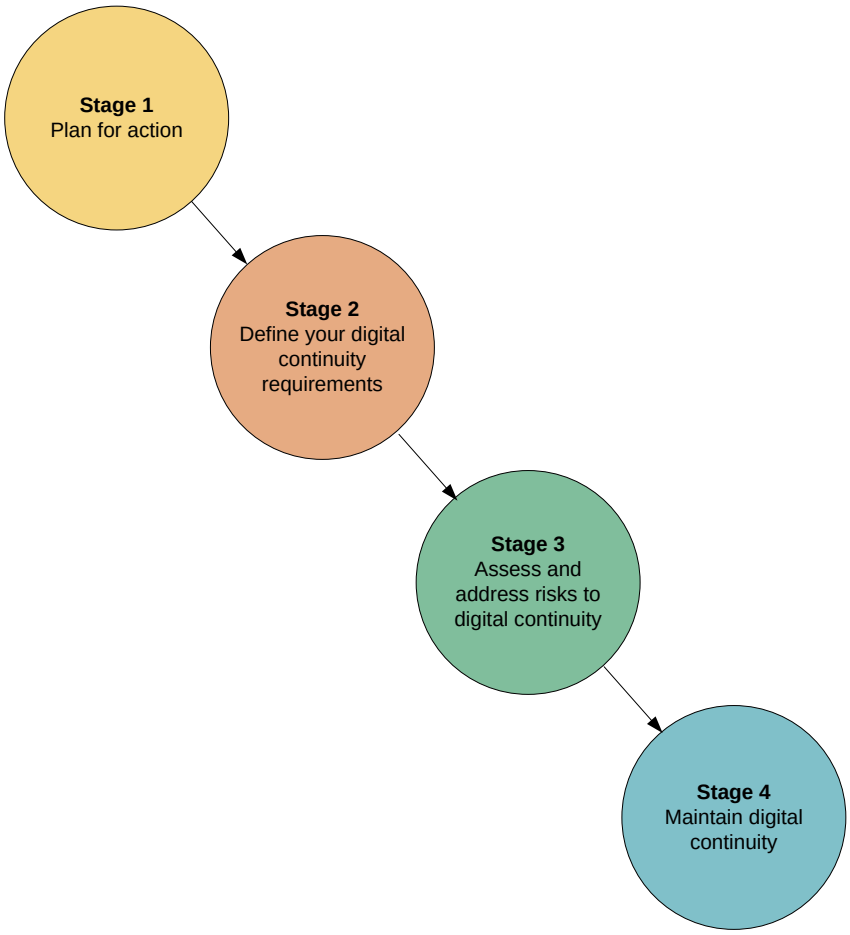

Figure 2: the four stage approach to digital continuity

You may want to use the four stage process outlined above to manage the entire change, or you may only want to use it as a checklist to make sure the key digital continuity issues and processes have been addressed within a wider change management process.

4.1 Stage 1: Plan for action

The first stage is to define the change that is going to occur. You should document and agree this with all parties involved. Note: this is the high-level change – you will consider the impact of that change on your information in the next step.

Change	Details
What is changing?	What is it at the moment? What will it be after the change?
Why is it changing?	What is the principle driver for the change? Are there any additional benefits?
When is the change taking place?	Is there a deadline for the change? Is there a timeline, can it be scheduled to coincide with other

	changes?
Who is involved?	Who is managing the change and who has sign-off? Who is involved directly? Who must be kept up to date?

It may be the change is fixed and you have no control over the scale and scope. However, it could be that in the process of defining the change (and going through the rest of the steps of the process) you are able to modify specific elements so that you can mitigate risk, minimise impact or take advantage of opportunities.

4.2 Stage 2: Define your digital continuity requirements

Once you have understood the change, you need to consider which of your information assets might be impacted, what their usability requirements currently are and how you must maintain or change those requirements.

Ideally you will have an IAR which lists all the information your organisation holds, grouped into manageable assets, each with an assigned owner and clearly defined set of requirements. You can use this register to check each asset and consider the potential impact, selecting out those assets which may be affected.

You must be sure to look beyond obvious impacts to track potential knock-on effects. There are likely to be complex relationships between information, technology and business needs so a variety of things may be affected indirectly. Examples of the types of changes and their impacts on how you use and support your information are provided in the Appendix.

For each of the assets potentially affected by the change you need to document their usability requirements, what they are currently, and what they must be after the change.

For each information asset affected	
The current usability requirements	How do you need to **find** it? How do you need to **open** it? How do you need to **work with** it? How do you need to **understand** what it is and what it is about? How do you need to be able to **trust** that it is what it says it is?
Any changes to the usability requirements	Specifically referencing the above requirements
Any changes to the technology that supports these requirements	If the requirements have changed, how does the technology need to change to support the new

	requirements?
Any changes to the business processes	If the processes have changed, are there any follow-on effects that will impact the business?

4.3 Stage 3: Assess and manage impact and risks to digital continuity

Once you have a comprehensive list of the requirements to maintain and/or manage those that must change, you should do a risk assessment looking at how the change may impact your information. Ask the following questions:

Risk assessment	
What are the risks?	Are there any risks new requirements will not be met, or that existing requirements will be compromised by the change?
Mitigations	How can we reduce the likelihood of each of these issues arising? Can we do anything before the event to reduce the impact of these issues if they do arise?
Testing	How will we know when and if the risk has been successfully avoided?
Contingency	If it is not avoided, what actions can be taken after the event to reduce the impact?

Your mitigating actions may involve knock-on effects on other areas of your organisation – for example, if a piece of technology which supports one of your usability requirements is decommissioned, an alternative piece of technology may have to be reconfigured so that it can take over support. You should liaise with representatives from across your organisation to negotiate follow on changes which are necessary to retain your usability. It may be that you have to find a compromise – that they are not able to support the changes you need, or that they insist upon changes that you would rather not implement. However, there may also be opportunities for savings and efficiencies – streamlining redundant technology or sharing resources with other parts of your organisation.

You must answer and agree the questions above in coordination with everyone involved – the people organising and performing the change and the people affected by it. You should document the risks carefully and assign specific owners. Mitigating actions should be incorporated into the overall plan for the project and tracked accordingly. The change should go ahead only once everyone is in agreement that all the risks are acceptable within the risk appetite of the organisation as a whole, and this project in particular. At this point you may need to return to stage 1 and refine the details of the actual change, maybe adjust the timeline to allow for more testing, or modify the scope of the change to allow a gradual rollout.

4.4 Stage 4: Maintain digital continuity

Through the risk assessment and requirements gathering, you should generate a list of actions to ensure your organisation maintains digital continuity. You should add these into the action plan and scheduling for the change process as a whole.

Once everyone is in agreement about the scope, actions and risks involved, the change can actually go ahead. This might be as instant as flicking a switch, or may involve several months of development, testing and integration. As the change goes through, you should monitor the risks log and ensure all the plans are actioned. You should ensure ongoing testing and assessment to allow issues to be flagged and addressed early, before they become too serious, or unfixable.

After the change, you should review the impact assessment:

- Have all the risks been avoided or the contingency actions taken?
- Have all the information requirements been met?
- Have you still got digital continuity?

You should also ensure the IAR, CMDB and any other relevant logs and documentation are updated.

You may not feel the effects of a change until a seemingly disproportionate amount of time after the actual change has taken place. You should retain and monitor the risk/impact assessments for long term sustainability. Finally, as part of the change management process, you should review the process itself after each change. Each change is a learning opportunity to further develop processes and understanding.

Appendix

5 Examples of change and their impacts

5.1 Business change

Changes in policy or legislation, changes in function, reorganisation and restructuring can all impact on how your business needs to use its information. This can prompt changes to different aspects of your usability requirements, or may require changes in ownership of information and where it is located and managed. Examples of changes to usability requirements for your information and the impact this can have are detailed below.

Business change often acts as a driver for further changes in technology and information management and ownership.

5.1.1 Changes to how you need to find your information

Changes to how you need to find your information can require both technology and information management changes.

Example business requirements	Impact
You need searching to be faster, it currently takes too much time to find information	You may need to change your technology, improve your search algorithm, or improve your hardware to allow faster processing
Search criteria need to be more flexible, you need to be able to search against more fields	This may be a technology change to allow you to record more fields, or enable you to make more complex searches. Or it may be an information management issue to update/introduce a metadata policy and train people to use it

5.1.2 Changes to how you need to open your information

This category covers not only how you limit access to your information, but also how you need or want to share it more widely.

Example of business requirements	Impact
You need to increase security and restrict who can access information	If you already have security measures in place which just need updating, this may be an information management issue to clarify roles and access levels.

	However, it may also affect technology if you need to enable new restrictions
You need to share your information with a wider audience as part of the government transparency agenda	The IAO, alongside the information management team can advise on promoting the sharing of the information. Datasets for example can be shared via data.gov.uk

5.1.3 Changes to how you need to work with your information

The way you work with your information is what you can do with it once it is opened, how you need to be able to use it. These issues tend to be largely technology related, requiring changes to software or configurations.

Example business requirement	Impact
You need to make a previously editable asset read-only so that it is no longer updated and can be archived	You may need to migrate file formats, either using existing software or using new technology to produce an archivable format. The information management team should have recommendations for how to archive information
You need to change the way data is gathered and entered into a database	You may need to make adjustments to the technology to enable you to record different information, for example adding fields to a database

5.1.4 Changes to how you need to understand your information

Understanding your information is largely about metadata – information about your information. Who created it, when and why? When was it last updated?

Example business requirement	Impact
You need to be able to track version histories of documents and reliably identify the latest	You may already be able to do this within your current technology environment, in which case it falls to the information management team to train people how to use it and encourage them to do so. You may, however, require technology changes to add the functionality to your systems
You need to be able to understand and evaluate your file formats to avoid technical obsolescence	The threat of obsolescence of information is now business critical, so you need to evaluate these formats in the context of your own business needs and technological environment

5.1.5 Changes to how you need to trust your information

Trusting your information is about being able to prove, to a defined level of confidence, that your information is what it says it is. The information management team should be involved in any changes to the tracking and reporting of audit information; you should ensure everyone in the organisation understands how their actions are being monitored.

Example business requirement	Impact
You need to be able to start tracking who has printed a file	Your information management team will need to develop the policy for what is being tracked and who has access to the reports. The technology team will then need to implement systems to do this
You need to be able to prove files have not been tampered with	If you have legal obligations, you must clearly understand what is required of your information so you can correctly and securely record it. Your business and legal teams will need to work closely with information managers to create the policy and work with the technical teams to implement and test the solutions

5.2 Technology changes

5.2.1 Software changes

The software applications used to create, access, manipulate and store most public sector information are constantly changing and evolving – if these applications no longer support the information you have previously created and still need, then you have a continuity problem. However, not upgrading particular pieces of software may mean that support is no longer available, or you are not able to share and re-use files from other organisations.

Example software changes	Impact
Updating to a new version of a key piece of software	You may no longer be able to access files created in the old version. The same update may mean that files created in the new version can no longer be shared with another organisation which is still using the older version. You must make sure that the new version of the software does not remove features which you were using, or break any customised add-ins which you rely on

Updating the operating system	The operating system not only has direct impacts upon the way information is used, but can have indirect effects on the way that it impacts other pieces of software that may not be available on the new platform, but are required for your information
Decommissioning legacy systems and old software, streamlining and consolidating IT systems	Information created using the decommissioned systems may not be accessible using other software. You may need to consider migrating data or file formats to maintain the usability of your information

5.2.2 File format migration

The Government has selected Open Document Format 1.2 as the standard for editable office documents to be used across government. You should evaluate the steps required to comply with this requirement to see how you can best and most easily support this implementation.

Either as part of a software change, or in isolation, migrating information between file formats has a number of risks associated with it. Even if the new format has 'better' support for your long term digital continuity, the process of migrating into it can cause a loss of digital continuity itself. For example:

Example file format changes	Impact
You need to migrate from a proprietary file format to another format such as an open one (maybe due to a software change)	The new format should be carefully evaluated before any migration is undertaken, it must support all the usability that is required and the migration must be done carefully to ensure no data or metadata is lost
A new file format is now supported by an established piece of software	The new format should be evaluated to consider whether it is 'better' to use or not. For example, although your organisation is using the new version of the software, other organisations with whom you share your files are not and they cannot open the new format

5.2.3 Hardware changes

Hardware is replaced on relatively well-planned schedules and lifecycles are documented and tracked to allow for long term planning of licenses, support requirements and budgets. Unfortunately, hardware changes also occur on short notice when systems fail. Disaster recovery plans should be in place to make sure that even these spontaneous changes are well managed and no information is lost. It is vital to include risks to digital

continuity into all these types of planning to protect your information through expected and unexpected change.

Example hardware changes	Impact
Phasing out support for legacy media types such as floppy disks, magnetic tapes, CDs and DVDs	Although new data is not being created on these formats, it may be that older files are still held on these
Introducing new hardware platforms to the organisation, for example Macs or smartphones	New platforms may not have support available for the software currently used to support the use you require from your assets

5.2.4 Technology management changes

The way you manage your technology affects the way it supports information. You must work with colleagues across disciplines to ensure you have an informed and consistent approach across your organisation. You should also avoid lengthy contract tie-ins or committing to contracts that make changes to meet new business requirements prohibitively expensive.

Example management changes	Impact
The license for a particular piece of software is allowed to expire	Rationalising the number and types of licenses is a good way to save money, however you must perform a full audit to make sure that no one is actively using the software and that there are no legacy or archived files which you may still need to access in the future which you will not be able to do if the license has expired
Reducing a support agreement from the top level to a mid-level, with corresponding decreases in response times	If a new support contract has lower response rates, in the event of a failure users will not be able to access their information for longer

5.3 Information management change

5.3.1 Ownership and governance change

Changes to your information governance structure, and roles accountable for owning information and risk, will prompt a change in how that information is managed. You need to ensure that you maintain an understanding of what information assets you have, and have a governance framework in place to manage risk and change. This challenge can arise when going through significant organisational changes and restructures, such as MoG change, when overall ownership of the information shifts.

Example ownership/governance changes	Impact
The asset is moved into a different department, a new group of people become the primary users and owners of the asset (this may be driven by a MoG change)	As information is created, changed and deleted from within the asset it is easy to introduce errors, for example incorrect or absent metadata, or corruption of audit trails. If the asset is moved into a different department, this may introduce risk as the technology and management processes change. You must ensure a full handover is given and the new users are correctly trained in how to use the information to prevent errors occurring. You must integrate the information asset into the new information and governance structures

5.3.2 Individual staff changes

Each information asset is connected to a number of people and may be dependent on particular expertise to understand the information and maintain its context and supporting technology. As these individuals come and go they can have a significant impact on the digital continuity of those assets.

Example people changes	Impact
The Information Asset Owner (IAO) leaves the organisation	The IAO is the primary custodian of the asset, responsible for managing risk and maximising opportunities. This is the individual who best understands the asset and its requirements and who should act as its advocate in times of change. If the asset owner changes, you can lose this understanding. If you do not replace the asset owner, or you poorly manage the handover, you have an increased risk of losing the digital continuity of your asset
The technology administrator for the system holding a key information asset leaves the organisation	Bespoke and legacy technology is often highly dependent on the skills and expertise of a small number of individuals who have built up specific knowledge of how technology works or information is structured and organised. There is risk to the ongoing usability of the information if you do not capture and share the knowledge and effectively hand it over through succession planning

5.3.3 Operational policy and process changes

Your organisation will have a number of policies and processes in place which inform how you should create, manage, share and discard information. The information management team should be responsible for both managing what is in those policies, but also for communicating and educating colleagues to make sure that operational processes are compliant with the policy. Policy and process changes may be driven from within or influenced by changes in wider policy and legislation.

Example policy/process changes	Impact
The organisation is introducing a new protective marking scheme and needs to ensure this information is captured in the Electronic Document and Records Management System (EDRMS)	Changes to the information you need to record about any given information asset will prompt a number of changes in policy and processes. You may need to update the EDRMS metadata policy to make it mandatory for staff to populate certain metadata fields. You may need to reconfigure the system to ensure it can capture and manage any new metadata required. You must train users on the new system
The security policy is being revised to restrict the number of people who can access key finance documents	You will need to implement changes to privacy settings and access levels. You may be able to do this using existing technology, or you may have to customise them
Transparency policy is being revised to require all published datasets are published in machine readable format	You may have to convert datasets from one format to another, or at the very least, their update their usability requirements in the IAR
Retention schedules is being reviewed and updated, changing the retention period for various information assets	You will need to update retention related metadata and disposal schedules associated with information. You might need to change technology configurations and settings. Users of the information will need informing of the changes, and potentially trained. If retention periods are significantly extended, you will need to review the technology you are dependent on against the usability requirements to assess risks to digital continuity over the new retention period