The National Archives

Digital Continuity for Change Managers

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.

Planning for change means managing your information and supporting technology in a way that leaves you better positioned to respond to inevitable changes with agility and flexibility, and in a way that minimises the risks that come with change. It means ensuring that digital continuity is reflected in your business plans and strategies as well as, policies and risk and change management processes.

1.1 What is the purpose of this guidance?

This piece of guidance helps you to understand:

- why your information is at risk during times of change
- what digital continuity is and why it is important
- how your digital continuity can be affected by change
- how you can make sure your information is protected

This piece 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.

No prior knowledge of digital continuity is required to read this guidance, although you may find the *Understanding Digital Continuity* document useful to expand your knowledge. Managing your digital continuity through change forms an important part of the final stage in a four-stage process: the wider management of your digital continuity. You can find out more about this process in *Managing Digital Continuity*.

1.2 Who is this guidance for?

This guidance is aimed at everyone involved with the planning and implementation of any changes that could affect the use or management of information. This may include project managers, change managers and risk managers, who may be either business or Information Technology (IT) focussed.

The information will also be useful for anyone concerned with managing information, information risk, or information assurance, e.g. KIM managers, IT managers, Information Assurance (IA) teams, Information Asset Owners (IAOs) and Chief Executive Officers (CEOs).

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

2 Digital continuity and change

2.1 What is digital continuity?

Digital continuity is the ability to use your information in the way you need, for as long as you need. If you do not actively work to ensure digital continuity, your information can easily become unusable.

Information is at the heart of good government, but without care and consideration the digital information on which government depends is less likely to survive and remain usable than paper records.

Understanding how you need to use your information is a key part of managing your digital continuity. What constitutes 'usable' will be different depending on your business' needs but in practical terms, your information is usable if you can:

- find it when you need it
- open it as you need it
- work with it in the way you need to
- understand what it is and what it is about
- trust that it is what it says it is

USABLE = AVAILABLE + COMPLETE

Usable: your information meets your requirements for how you want to use your information.

Available: you can find what you need and you have the correct technology to open it and work with it in the way you need.

Complete: everything you need to use, understand and trust the information is present, including the content, context and all the necessary metadata.

2.2 Why does it matter?

Managing digital continuity is essential if you are to protect the digital information you depend on to do business. This enables you to operate accountably, transparently, legally, effectively and efficiently. It helps you to protect your reputation, make informed decisions, 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.

Once you have lost digital continuity, it is very difficult and often impossible to restore it – and if you do manage to, it can involve severe financial and reputational repercussions. It is much more cost and time efficient to ensure you do not lose it in the first place.

2.2.1 Supporting wider government agendas

It is your duty to maintain the accessibility and use of the public record, and managing digital continuity will help ensure this. Usable information is a prerequisite for working collaboratively and efficiently – no government department can afford to waste its resources on recreating or recovering lost information.

The need to ensure digital continuity is clearly recognised and embedded into wider government priorities and agendas on transparency, information management and information assurance. For example, it is included in Section 46 Code of Practice, the National Information Assurance Strategy, the Information Assurance Maturity Model and Assessment Framework, and in the government's response to Sir Alex Allan's review of its strategy for managing digital records and archives, 'Better Information for Better Government'.

2.2.2 Realising savings and efficiencies

You can realise savings and efficiencies through providing the right level of continuity for the right information. Ensuring digital continuity can deliver real efficiency benefits, bringing opportunities to dispose of the information and IT that you do not really need, reducing data volumes and streamlining your technical environment.

2.3 Why does change affect digital continuity?

The digital continuity of your information is maintained when your technology and information management processes support your information assets in meeting your business requirements both now, and in the future. This occurs 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 process enables you to use your information, and is agile enough to cope with your changing requirements

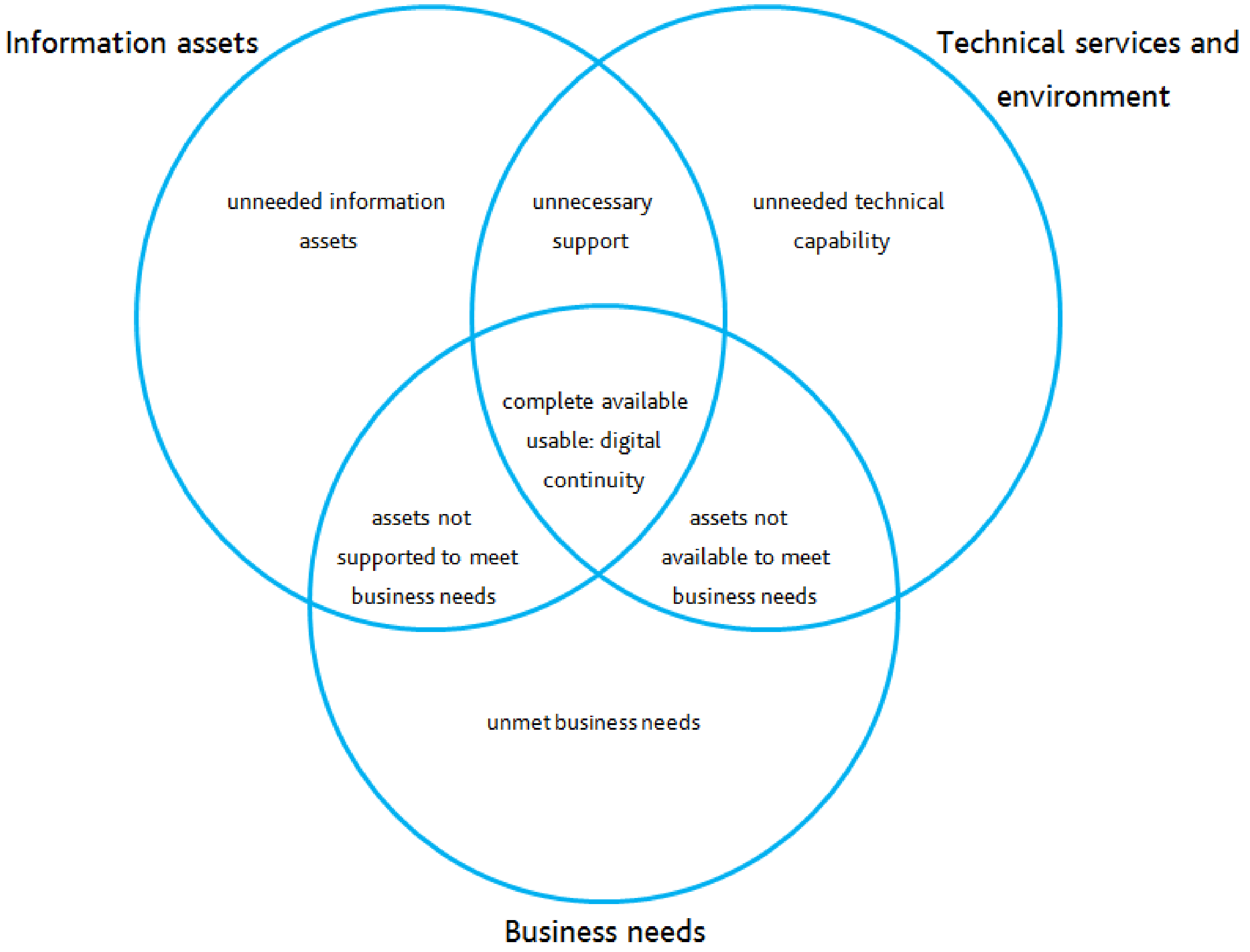
Information assets
Technical services and environment
unneeded information assets
unnecessary support
unneeded technical capability
complete available usable: digital continuity
assets not supported to meet business needs
assets not available to meet business needs
unmet business needs
Business needs

Figure 1: ensuring digital continuity

Managing change is key to managing digital continuity. As shown in the diagram above, digital continuity is about the alignment between your information, your usability requirements and the complex technological environment which supports it. Changes to any of these elements, even seemingly minor ones, could have a dramatic impact on your ability to use your digital information. Managing change means identifying when your information might be affected by a change, undertaking impact assessments to understand where there might be risks to your digital continuity, and putting in place effective plans to make sure your information remains usable through the change.

If changes are not effectively managed, you could be left with information assets you can't use, or technology that fails to deliver the support in the way your information needs. At best, this creates inefficiencies. At worst, it can result in the loss of the information you need.

It's not only immediate changes that you need to think about, there is also the risk that you are unprepared for change in the future. You should consider how you will want to use information, for instance in five years' time – are your business needs likely to change? Have you planned the lifecycle of your hardware and software so that you know when change is likely and can plan your strategies for maintaining digital continuity in advance? You should also have succession plans in place, so you have some contingency if staff critical to managing your information and IT leave the organisation.

3 How to manage digital continuity through change

3.1 Who you need to talk to

To effectively protect your information through change, you will need to work alongside a number of people in your organisation. Your information management team and the relevant IAOs will be able to provide guidance on what information you have, how it needs to be used and what risks are associated with it. If you have a Senior Responsible Owner (SRO) assigned to manage digital continuity, they will also be able to provide advice and assistance. Depending on the scale of the change, you may need to include the CEO in your communications.

There may be resistance to change, when it has a negative impact upon assets and the ways they can be used. Liaising with asset owners and end users should be a dialogue and compromises may have to be made on both sides of the process. By engaging in this discussion early in the change process it will hopefully be possible to mitigate risks before they develop into issues which are more difficult to resolve. At the very least you will have a shared understanding and decisions can be taken from an informed position.

These conversations may also reveal opportunities to group additional changes together to minimise overall disruption. You may have opportunities to streamline information assets and the technology environment, revealing potential efficiency savings and system simplifications.

3.2 Impact assessment

For any change you must make sure an impact assessment is undertaken for your organisation's information assets, to establish how the change will affect how your information can be used. You may have to produce this yourself, or you may need to make sure your information management team is doing this. You should embed this impact assessment into your organisation's change management processes.

You will need to put together a comprehensive list of the assets that are affected by the change and how they are impacted. Ideally your organisation will have an *Information Asset Register* (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 of the change upon it, highlighting the ones which may be affected.

You must be careful to look beyond obvious impacts. There are likely to be complex relationships between information, technology and business needs so a variety of assets may be affected indirectly. Each asset that's affected may in turn affect other assets, technologies and business requirements, so what may seem an isolated change may in fact set off a chain reaction through a number of assets and systems. You can also use one vital change as a catalyst for other voluntary changes – either to improve services or to realise savings and efficiencies.

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

By the end of this identification process you should have a comprehensive, documented list of:

- the information assets affected by the change
- the current usability requirements of those assets – how you **find**, **open**, **work with**, **understand** and **trust** them
- any changes to those usability requirements
- any follow on impact to the technology that supports these requirements
- any follow on impact to the business processes
- any follow on impact to other information assets

Once you have identified these issues, you can include them into your planning alongside your other requirements, risks and actions. Depending on the scale of the impacts you may wish to include relevant IAOs, or the digital continuity SRO on your project board, on your communications list.

3.3 Risk assessment

While your impact assessment focuses on the planned changes and their impacts, you should also perform a risk assessment to consider and document the unexpected impacts. You must consider your information assets during this stage as well, to make sure that you are prepared as far as possible for what to do if things do not go as planned.

Part of the risk assessment will include creating an action plan to mitigate risks; things which can be done in advance to minimise the chances of incidents occurring, or reduce their impact if they do. You must work alongside the information management team and IAOs to develop this process and make sure it is communicated appropriately to everyone who uses the assets. See our *Risk Assessment Handbook* for more information on performing a digital continuity risk assessment.

3.4 Acceptance testing

For major change with either significant impact, or considerable risk, to information assets there should be an agreement during the planning stage of how to assess whether the change has been successful. These checks should be incorporated into your test plans. You should also make sure that all relevant documents, registers and logs are updated to reflect the change.

4 The impact of different types 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 4.1)
- Changes to the technology that supports the information (section 4.2)
- Changes to the way the information is managed (section 4.3)

Each of these types of change is likely to have different types and levels of impact on the information your organisation holds and uses. You may be responsible for one particular type of change, or your project may have wide ranging effects covering multiple categories.

4.1 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.

With business changes, it is vital to first understand what your starting point is. If you have an IAR, this should provide detail on your information assets and the usability required from them to meet your business objectives. We give some examples below of the potential impacts of changes to these usability requirements.

4.1.1 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 requirement	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 a greater number of fields	This may be a technology change to allow you to record a greater number of fields, or enabling 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

4.1.2 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 business requirement	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

4.1.3 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	You may need to make adjustments to the

entered into a database	technology to enable you to record different information, for example adding fields to a database

4.1.4 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 version	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

4.1.5 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

4.2 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 obsolescent 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.

The usability requirements of the information are generally delivered by the technology environment – it provides the tools that enable the information to be found, opened, worked with, understood and trusted. Any changes to the environment can therefore have very immediate and direct effects on the ability to use the information in the way that business requires. Changes to one piece of technology may also have knock on effects on other pieces, which in turn affect more information assets. Ideally your organisation's technology team will have a Configuration Management Database (CMDB) or similar register which will describe the relationships between systems and tools.

4.2.1 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 in 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,	Information created using the decommissioned

streamlining and consolidating IT systems	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

4.2.2 File format migration

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)	You should carefully evaluate the new format before you do any migration, as it must support all the usability that is required. You must undertake any migration carefully to ensure no data or metadata is lost
A new file format is now supported by an established piece of software	You should evaluate the new 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
You need to comply with the UK Government standard for editable office documents to be used across government 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

4.2.3 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	Although new data is not being created on these

floppy disks, magnetic tapes and CDs	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.
Use of cloud based services to replace hardware	Security arrangements and Service Level Agreements (SLAs) that need to be put in place to manage differently to onsite services

4.2.4 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
Vendor lock-in or reliance on a single provider	Ability to retrieve and migrate information in a cost effective way. If a smaller provider – what happens if go out of business?

4.3 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, metadata policies and IARs. There may be a dedicated team to manage information, with networks and extensive support for IAOs. Whatever process 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. There are tangible things such as passwords which must be transferred, but there is also a lot of knowledge which can be harder to transfer – understanding of how information was gathered, where things are kept, or how to use bespoke software. Information may also be stored inside email accounts and on local hard drives which may no longer be accessible once the person leaves. You should work alongside the HR department to make sure the exit process includes information management concerns.

4.3.1 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

4.3.2 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

4.3.3 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	You will need to implement changes to privacy

number of people who can access key finance documents	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 are 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

5 Next steps

There are two facets to managing your digital continuity through change. Firstly, you must make sure that information management is embedded within your existing change management processes, and also that your impact and risk assessments and test processes include considerations for the information that supports your business and relies on your technology. Secondly, for each individual change you must engage with your organisation’s information management team and relevant users of the information assets. Communication is key to protecting your information and potentially finding additional savings and efficiencies.