The National Archives

Incorporating Digital Continuity into your IT strategy

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.

© Crown copyright 2017
You may re-use this information (excluding logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence or email psi@nationalarchives.gsi.gov.uk.
Where we have identified any third-party copyright information, you will need to obtain permission from the copyright holders concerned.
This publication is available for download at nationalarchives.gov.uk

Contents

1 Introduction

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

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 guidance will support Chief Information Officers (CIOs) and Chief Technology Officers (CTOs) to embed digital continuity into the organisation's Information Technology (IT) strategy.

You should already understand the basic principles of digital continuity and recognise the need to manage this within your organisation. Your organisation may also have mapped the technical dependencies of your information assets. This guidance will support you in maintaining your digital continuity over time and through change, which is the final stage of our four-stage process of managing digital continuity.

Specifically, this guidance will help you to understand the principles to follow when including digital continuity in the planning and development of your IT infrastructure. It will reduce your chances of encountering digital continuity issues in the future, and ensure you are well placed to respond to changes in the way you need to use your information.

2 Digital continuity and your IT strategy

Digital information is vulnerable at times of change. Your organisation relies on technology and systems to enable it to use its digital information as it needs to; providing the ability to find, open, use, understand and trust your information.

If your technology environment changes, your organisation may no longer be able to use its digital information in the way it needs. To maintain digital continuity, you must ensure your technology infrastructure is based on planned development and change, rather than ad hoc response to demand, new technology or changing business priorities.

However, establishing digital continuity in your existing IT strategies will also enable you to better respond to any changing requirements as they do arise, ensuring information does not become contained in silos and that you have the interoperability and flexibility necessary to meet these changing requirements.

2.1 Why is embedding digital continuity in your IT strategy important

It is difficult to restore continuity when it has been lost. Our *Managing Digital Continuity Loss* guidance can help you in these circumstances; however restoring continuity can be expensive and is not always possible. The best mitigation against losing your information is to manage the relationship between your information and technology well in the first place.

Your organisation needs to make a commitment in its IT strategy to support digital continuity: enabling the digital continuity Senior Responsible Owner (SRO) to plan and manage digital continuity, undertaking a digital continuity risk assessment and embedding digital continuity principles into the policies and processes covering your technical environment.

Digital continuity is also central to meeting your business continuity and information assurance requirements and supports government agendas.

2.1.1 It supports business continuity

To ensure business continuity, your organisation needs to plan for the ability to use its digital information over the long term. While business continuity involves planning for the restoration of access to key digital information following an incident, managing digital continuity also mitigates the risk to the degradation of your digital information over time and through change.

2.1.2 It supports information assurance

Losing the ability to use your digital information in the way that you need to is an information risk like any other, and ensuring you can continue to use your information over time and through change is an important part of assuring and protecting it. Digital continuity forms part of the government's Information Assurance Maturity Model (IAMM).

Digital continuity guidance is available to support you to assure the availability and integrity of digital information through business and technology change.

2.1.3 It supports government agendas

IT strategies need to reflect that the way government is managing its services, producing and sharing information. It is important to reflect that the way that this information is being consumed is changing rapidly; for example, government emphasis on transparency and openness are reflected in the need to publish increasing amounts of public data. This makes it all the more important that you manage the digital continuity of your information; to ensure you can find, interrogate, trust, share, re-use and publish it as required. You should embed digital continuity principles into your IT strategy so that your organisation can take steps towards assuring the usability of its information.

3 Embedding digital continuity principles

The following principles will help you to manage your IT strategy in a way that supports digital continuity:

3.1 Build digital continuity requirements in your technology lifecycle

Information has a lifecycle that is different to that of the technology in which it is created or stored. If you do not consider this and plan the development of your architecture around retaining the usability of your information, your technology may stop you working with your information when you need to, in the way that you need to.

The most important time to think about how you will need to use your information is before development or procurement; it is much more expensive and difficult (indeed, if possible at all) to fix these issues after development is complete or a product has been rolled out. There are three key issues to consider:

3.1.1 Procurement/systems development

Can you get information in to – and out of – the system, with its associated metadata? This may include user generated metadata, system metadata, audit logs etc.

You need to consider the following requirements **when developing or procuring new systems** – and ensure that any upgrades or fixes do not adversely impact on these:

- How does your organisation need to work with the information across its lifecycle and how will you ensure this?
- Can information be imported into or retrieved from the system during the normal operational lifecycle for use in other systems? (e.g. in some systems, standard metadata may be exported but user-generated metadata that was specific to the system does not get exported)
    - Can you use open standards for your information?
    - What interfaces do you need the system to provide to help you get at the information it holds?
    - What are your performance requirements for getting information in and out of the system?
    - Can you maintain the link with your metadata and audit information when moving information between systems or upgrading?

3.1.2 Decommissioning

Do you have digital continuity plans for each decommissioned system? This will need to include:

- What information do you need to keep?
- What are your usability requirements?
    - How are you going to ensure that usability requirements are met?
    - Will you need to retain the full functionality for your legacy information, or can you use cheaper formats or applications with less continuity risk? (e.g. can you convert legacy information into PDF, or use rendering technology rather than full applications?)
    - Can you use cheaper and more cost-efficient storage for the information you need to keep?
- How will you test for continuity after the change?
- Are you ensuring you dispose of information that is no longer required?

3.1.3 Interoperability

You should consider interoperability across your IT environment, including technology supplied by third parties, to ensure that information can be transferred between systems to support business use and digital continuity. It is important that you consider digital continuity in Service level Agreements (SLAs)/contracts if using third party providers or Cloud services.

Also consider how you can ensure maximum interoperability with your current technology environment.

- For infrastructure technology, it may be worth using existing or highly standard software, and adapting your business processes to fit the technology. This will require less specialist support and knowledge and is likely to be more compatible with other systems
- For strategic technology (with a unique business benefit), complex or non-standard technology may be the most suitable option, implementing the exact business processes you want, but with reduced chance of interoperability with other systems

3.2 Understand and manage your IT services

Your technology must support the provision of information that is complete, available and usable to the business. To maintain this, it is vital that you understand each of the elements of the technical environment which support its usability.

To monitor this, link your IT strategy to business services. You need to reflect these services in your technology lifecycle and technology architecture, and map them through an IT service catalogue.

The actions below will support you to monitor and manage your strategic priorities. You should:

3.2.1 Understand your requirements

You need to know what information is required by each business service and where that information is stored. You also need to understand the business value of that information. Use your *Information Asset Register* (IAR) to understand what information you hold and how the technology needs to support this.

This should also inform your technology decisions from the perspective of the organisation – e.g. at times of business change, development, upgrades, or new technology.

3.2.2 Build comprehensive configuration management

A planned and managed IT service is more likely to deliver digital continuity than one that develops reactively over time. Ideally your organisation will work towards having a comprehensive configuration management database and single enterprise architecture.

For digital continuity purposes, this will document the relationships between your information and technology architecture, including dependencies, and making the impact of change easier to measure and manage. It will support you in implementing robust change management and configuration management, enabling you to maintain the usability of your digital information.

3.2.3 Manage your architecture

Building an understanding of digital continuity and how you need to use your information over time into information architecture, technical architecture or a single enterprise architecture will enable the organisation to develop an IT environment which supports the business use of information across its lifecycle.

3.2.4 Establish governance

To ensure you have digital continuity embedded in your IT policies and processes, you need to assign owners, ensure they are implemented and that you have a process in place to ensure compliance.

Also include Information Management (IM) professionals on change boards to ensure that the impact of change on the way the organisation can use its information is being considered.

3.3 Streamline and standardise your technical environment

For many organisations, their technical environment has developed over time according to demand, new technology or changes in business priorities. Ad hoc growth often results in a diverse and complex technical environment that is difficult to manage and has not been planned to meet usability requirements, including interoperability between systems. This makes it increasingly difficult to ensure you are able to use your digital information as you need to, and that you are managing digital continuity through comprehensive change and configuration management.

Reducing the complexity of your current technology infrastructure could mean:

- less complexity to manage over change
- reduced costs by disposing of unnecessary licences, support contracts and storage
- increased flexibility as standardised information and technology allow for greater interoperability
- less reliance on specialist knowledge and skills

3.3.1 Review your use of open standards

Open standards enable the transfer of information between systems more easily and broaden the choice of technology available, avoiding lock-in to proprietary formats. This provides flexibility for the sharing and significantly increases the likelihood that your information can be used in the future.

The Cabinet Office has issued guidance on the use of open standards in government.

Open standards may not always be the most appropriate choice for your business function; however you should always ensure that your information standards are as open, commonly used or standardised as possible.

3.3.2 Limit your use of different file formats

Reducing the complexity of the IT environment by minimising the number of systems, applications and formats in use will reduce overheads, make change easier to manage and improve interoperability. Active management of file formats used by your organisation, including maintaining a file format policy that identifies the recommended or enabled file formats, will help you to:

- maintain control over your IT environment
- ensure that applications are in place to provide ongoing access to all information
- more effectively plan for file format migration and conversion when necessary

3.3.3 Reduce reliance on legacy technology

Legacy technology increases risk to digital continuity because it reduces your ability to respond to change, making it increasingly difficult and costly to maintain and resolve issues that arise. It also tends to be harder to extract information from legacy technology, often held in non-standard formats or structures. The longer legacy technology is left in place, the higher the risks and harder it will be to move away from.

Consider limiting your use of legacy formats, especially those which may be going out of support. You should consider this in conjunction with representatives from the IM function in order to ensure that you are applying the right level of digital continuity according to the business need.

You may still need full functionality from your legacy formats, for example maintaining the ability to edit, change or re-use the information. If this is the case, consider the costs, benefits and risks associated with conversion against the cost and risk of continuing to support the full application. In many cases it will be sufficient to use viewer (or rendering) technology rather than the full application, which reduces the risks to digital continuity and is cheaper.

3.3.4 Reduce data volumes

Managing your data effectively and removing unnecessary information will reduce your overall volumes. This will make it easier for your organisation to find and manage the information it needs and reduce costs and complexity associated with maintaining its digital continuity over long periods. It will also reduce your storage costs and consume less energy in heating and cooling your servers, supporting you to meet the green agenda. If you use a third party IT storage supplier, you may find that cost savings are reflected at the time of re-contracting.

4 Next steps

Now you have recognised the need to embed digital continuity in your IT strategy, you need to ensure that this is reflected in the right places. You will need to embed digital continuity into relevant business plans, procurement policies, architectures, requirements and specifications, checklists for introducing and decommissioning technology, change and risk management policies and strategies. You must ensure these have ownership at the correct levels and compliance is monitored.

You also need to talk to your IM team and reference their strategies for digital continuity within your own technology strategy and processes, ensuring cohesion.