The National Archives

Embedding Digital Continuity in your IT Environment

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 digital 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 Who is this guidance for?

This guidance is aimed at Heads of Information Technology (IT). It will help you to ensure all the component parts that make up your IT environment work together to maintain the digital continuity of your information.

Corresponding guidance in *Incorporating Digital Continuity into your IT Strategy* provides a more high-level guide on why and how to embed digital continuity within an organisation's overall IT strategy.

1.2 What is the purpose of this guidance?

This guidance will support you to embed digital continuity thinking into your organisation's IT operational management. It details the overarching principles that are required to ensure that you are embedding digital continuity in the design and management of your IT operations.

By embedding digital continuity into your IT operational management, you can ensure you are well placed to reduce your chances of encountering digital continuity issues in the future, and ensure you are able to respond to future challenges in the way you need to use 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. 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 identified its business requirements and the services it needs to provide, and mapped and recorded the information assets and the technology supporting these services. 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.

2 Building digital continuity requirements into the technical lifecycle

Information has a lifecycle that is different to that of the technology in which it is created or stored. The use that business needs from its information will often outlive the technology that is currently supporting it. An IT strategy has to cater for these overlapping lifecycles. 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 it in the way that you need to. As Head of IT, it is your responsibility to ensure that your IT is supporting your business services. You do this by the active management of an IT Service Catalogue (see Section 3.2)

2.1 Procurement supplier management

Information assets age rapidly; data volumes can double every few years and technology changes at a faster rate than ever before. Establishing an *Information Asset Register* (IAR) in an ICT Services Contract enables all parties to maintain a shared understanding of the information and its required business use so that the impact of change may be assessed and mitigations agreed where necessary.

See *Digital Continuity in ICT Services Procurement and Contract Management* for more detail.

2.2 Systems development and testing

It is important to plan for digital continuity when designing new systems and enhancing existing systems. You must develop front-end applications and back-end databases in accordance with best practice guidelines.

The availability and usability of business information (e.g. through applications, databases, websites) is affected by the quality of development and testing undertaken. It is important that you include provision for digital continuity requirements into all development and testing (usability, regression and security) procedures and processes.

For more information about managing your technical infrastructure as well as your IT strategy, see *Incorporating Digital Continuity into your IT Strategy*.

2.3 Embed into your technical architecture

Technology needs to support the business and not drive the business. Developing an enterprise architecture entwines your information architecture with your technical architecture. Mapping your IT services and IT systems to the business services and information they support will enable effective management of your technology lifecycle and technical architecture. This is best tracked through the creation and management of a Configuration Management Database, which captures the relationships and dependencies over time between IT components and the people, processes and business services they support.

2.4 File format migration

The information your organisation needs will be held in a variety of formats. Each individual piece of information may itself be held in several formats so that it can meet a number of usage requirements. When converting file formats you will either:

i. Need to replace one format with another. For example, this may be due to changes to the software tools that are used in your organisation, a move away from legacy formats that are at risk of obsolescence, or changes to the standard format your organisation uses to publish online.
ii. Need to create an additional version in a different file format to meet your usability requirements. For example, a brochure was created in a desktop publishing format, but it must be converted into an additional format which can be published online.

There are a number of different drivers for each type of conversion. You should review your file formats periodically to assess whether any of them hold risks to your information. You can also pro-actively convert file formats to reduce the risk of digital continuity loss.

Maintaining the digital continuity of your information means ensuring it is complete, available and usable, over time and through change. It means making sure that your business has the information it needs, and that the technology enables the information to be used in the way business needs it to be. To maintain your digital continuity you may need to convert file formats, as file formats naturally age and can become more risky, but also because your business may change how it needs to use its information, or because your technology environment changes.

If you do not pro-actively convert your formats, you may find that you are no longer able to access or use your information in the way that you need, or that to do so you are locked in to using particular pieces of software. However, when replacing formats you may be planning to remove support for the older file formats, and potentially deleting the original files altogether, which holds its own risks – so you must make sure your process and testing are comprehensive.

The National Archives' file profiling tool DROID can help you to understand what information you have, where it is, how old it is and technical information about the format.

3 Understanding IT services

3.1 Understanding your business 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 IAR to understand what information you hold and how the technology needs to support this.

See *Identifying Information Assets and Business Requirements* for guidance on identifying and recording the business requirements of the information you have.

3.2 Developing an IT Service Catalogue

IT services are made up of information assets, people, processes, procedures, documentation, and technical components. These should be managed and monitored through the provision of an IT Service Catalogue, Service Level Agreements and using your IAR. As you develop your catalogue you should endeavour to standardise and simplify your environment wherever possible, considering open standards and decreasing the reliance on bespoke or legacy systems. For more information on this please see Incorporating Digital Continuity into Your IT Strategy.

3.3 Configuration management

Configuration management is the process responsible for maintaining information about individual components required to deliver an IT service, including their relationships with one another. A configuration management system is a set of tools and databases that are used to manage your IT services' configuration data.

Developing a configuration management process with a configuration management system to support it is an important step towards achieving digital continuity, as you will be able to accurately understand and track the relationships, dependencies, costs, risks and impacts to all business information and the technical and non-technical components that deliver this information.

4 Managing IT services

4.1 Your team

Your greatest assets, but also your biggest risks, in your technical environment are the people that design and maintain your IT systems and services. The risks from staff changing jobs or leaving your organisation are ever-present. The ability to maintain an understanding and control over your IT systems through this constant change is critical. You need to consider the importance of:

- creating and maintaining support and configuration documentation (see section 3.3)
- technical training
- system handover training
- maintaining awareness of this through training sessions and good communication

4.2 Multi-disciplinary working

Communication and awareness is essential in achieving digital continuity. In practical terms, IT and IM teams must break out of their traditional silos and learn to work together. Technology must support business needs and deliver and protect business information.

Shared management controls such as the IAR and the IT Service Catalogue are critical in achieving this wider awareness and joint control. Change boards (e.g. IT Change Advisory Board) are other crucial management controls where IT and IM managers need to share digital continuity risks and issues. As Head of IT, you must ensure that all IT boards (e.g. Change Advisory Board) have an information management specialist on them, and you should seek to ensure that all information management boards have an IT representative on them.

4.3 Project management

Structured business change (e.g. resulting from Machinery of Government changes, or annual business planning reviews) needs to be planned and implemented through programme and project management. Project managers can build digital continuity requirements into business change initiatives, including them within:

- project plans
- stage reviews
- work packages
- risk logs
- escalation procedures

You will also need to establish a clear digital continuity responsibility within a project team's roles (typically would expect to be within the IT and IM role on the project team).

4.4 Change management

Change management is the process responsible for controlling the lifecycle of all changes. The primary objective of change management is to enable you to make beneficial changes, with minimum disruption to the delivery of business services. 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. This means ensuring that digital continuity is reflected in your business plans and strategies as well as policies and risk and change management processes.

See *Digital Continuity for Change Managers*.

4.5 Service management

IT Service Management is a process developed in order to align the delivery of IT services with the needs of the business. This is reflected in Service Levels Agreements (SLA) with supporting Operational Level Agreements (OLA). You need to make sure that digital continuity is built in to the OLA that underpin agreed service levels with customers. You also need to make sure all SLA and OLA are included in a configuration management system.

5 Next steps

5.1 Developing a single enterprise architecture

Having a single enterprise architecture will enable you to support decision making during business change. An enterprise architecture brings together business models (e.g. process models and technical models (e.g. systems architectures or data models), which makes it easier to trace the impact of organisational change on the systems, and also the business impact of changes to the systems.

Developing a single enterprise architecture also helps define the critical architectural elements and the dependencies between them. Applications based on these models can then query the underlying architectural information, providing a simple and strong mechanism for tracing strategies to organisational and technological impacts.

Used in conjunction with an IT Service Catalogue and a configuration management system, it will also provide support for:

- re-use and innovation
- identifying efficiencies in workloads and roles
- the sharing and transparency agenda
- simplification of processes and procedures
- standardisation of technology (de-cluttering and reducing complexity)