The National Archives

# Managing Digital Continuity

# Stage 4: Maintain digital continuity

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.

**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.

## Introduction to Stage 4

This guidance explains the ongoing process of embedding digital continuity in your organisation's business processes and strategies in a way that maintains the usability of your information.

We have a four-stage process to help you manage digital continuity:

1. Plan for action
2. Define your digital continuity requirements
3. Assess and manage risks to digital continuity
4. Maintain digital continuity

In *Stage 3: Assess and manage risks to digital continuity*, we helped you to manage the risk of losing digital continuity by setting out governance and risk management structures, assigning responsibility for the management of risk, and assessing your current level of risk. This guidance deals with Stage 4 of this process, which comprises the following actions:

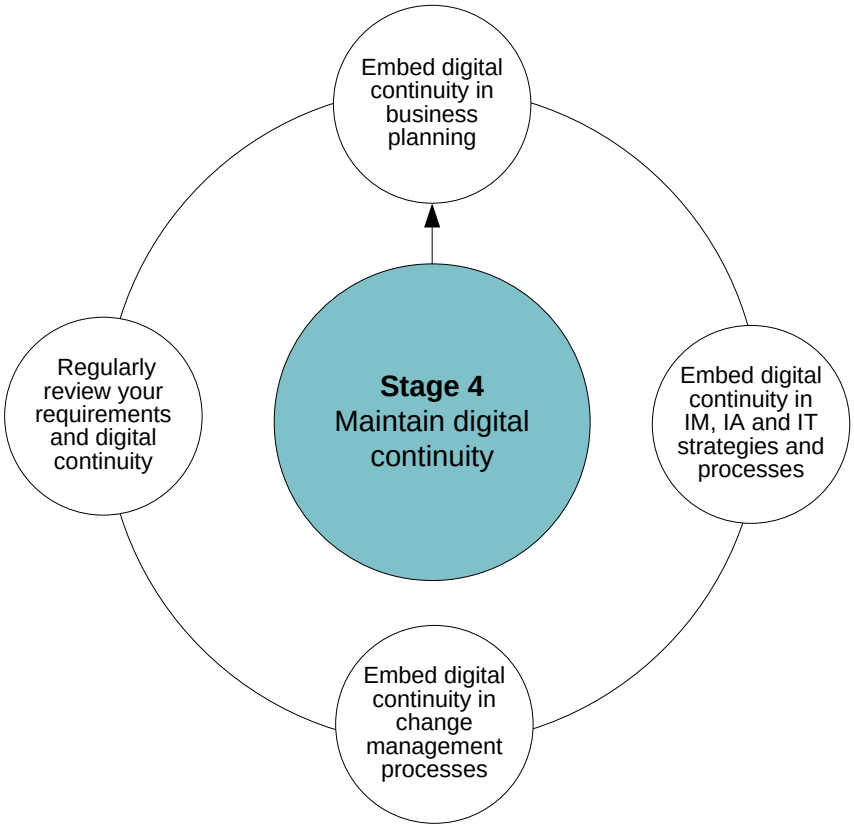


Figure 1: maintain digital continuity

To ensure you can continue to use your digital information in the way your business needs, over time and through change, you need to embed the concept firmly into your existing business processes and strategies, as well as keeping it in mind during planning stages of new projects. It is important to take a whole organisational approach to maintaining continuity and continue to involve different teams, such as Information Management (IM) and Information Technology (IT), on an ongoing basis. You should also ensure you plan for change.

## Actions to take

### 1. Embed digital continuity requirements in business planning

- Consider digital continuity in your strategic development plans and the implementation of new projects across the business, including new information systems and technologies, procedures and ways of working and changes to meet legislative requirements
- If digital continuity is considered properly in the planning stages, you could realise savings and efficiencies through providing the right level of continuity for the right information. This will enhance your ability to use and re-use your information, make it cheaper and easier to maintain information and avoid the need to take expensive mitigating actions in future

2. **Embed digital continuity requirements in IM, IA and IT policies and operational management**
   To ensure you retain usability of your information, you need to embed digital continuity in the management of your information assets and in your IT systems, strategies and service management.

You can maintain the digital continuity of your information assets by:

- **Managing their context and audit data.** Improving metadata or content may make them easier to find, migrate and manage
- **Implementing policies for managing the location of your information.** Optimising search tools so the organisation can easily locate and identify even information assets which are unstructured or in a hard-to-find location
- **Implementing policies for managing the access of your information**. Access includes managing passwords, access controls and encryption
- **Embedding digital continuity into service delivery processes and related policies** such as Service Level Management, continuity planning and capacity planning
- **Reflecting the usability you need** from your information in business planning, architectures and procurement cycles
- **Building a consideration of the long-term use of information into IT system design and development**, to minimise the impact and cost of change
- **Including the need to maintain the usability of your digital information assets in contracts with IT service providers**

3. **Embed digital continuity in your change management processes**

- Ensure change policies and processes include assessment of the information risks that arise in the event of changes to business requirements, technology or organisational structures
- Add 'risk to loss of digital continuity' to your change management, project and programme risk registers as appropriate
- Include a digital continuity impact assessment in the planning and implementation of change projects. This must consider whether business change, technical environment and the way assets are managed impact on the usability of the information
- Ensure that your IT suppliers undertake a digital continuity impact assessment before making changes that could affect the information assets they manage or that depend on the technology they provide

- Plan and implement mitigations for any risks you identify through these processes to ensure that the usability of your information assets is not affected by the change
- Test the digital continuity of affected information assets following any changes – can you still use the information asset in the way you need to?

### 4. Regularly review risks and digital continuity requirements

- Monitor the progress of the mitigating actions planned during the risk assessment to manage risks to digital continuity to ensure they are appropriately implemented and have been effective
- Incorporate digital continuity into your Information Risk Policy and risk management processes
- Maintain a schedule of risk assessments and mitigations for each individual information asset
- Develop procedures to periodically test that the accessibility and usability of information assets meets your stated business requirement, testing whether or not you have maintained digital continuity, the effectiveness of mitigations, and whether it faces new risk
- Establish a process for the systematic and regular review of risks to the digital continuity of your information assets as part of their lifecycle management.
- Manage digital continuity incidents and problems through your information assurance incident and problem management procedures, and include them in your incident reporting and metrics

## Next steps

You can find more detail on the individual aspects of maintaining digital continuity, such as managing digital continuity through change, using other pieces of guidance on The National Archives' website.