The National Archives

Managing Digital Continuity

Stage 1: Plan for action

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 1

This guidance is to help you get started in managing digital continuity. It will help you establish your objectives, who you need to work with, and how to manage digital continuity across the organisation.

In *Understanding Digital Continuity*, we provided you with an introduction to help you to recognise the need to manage digital continuity in your organisation, highlighting the risks and opportunities this process can bring.

We also introduced the idea of 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

This guidance deals with Stage 1 of this process, which comprises the following actions:

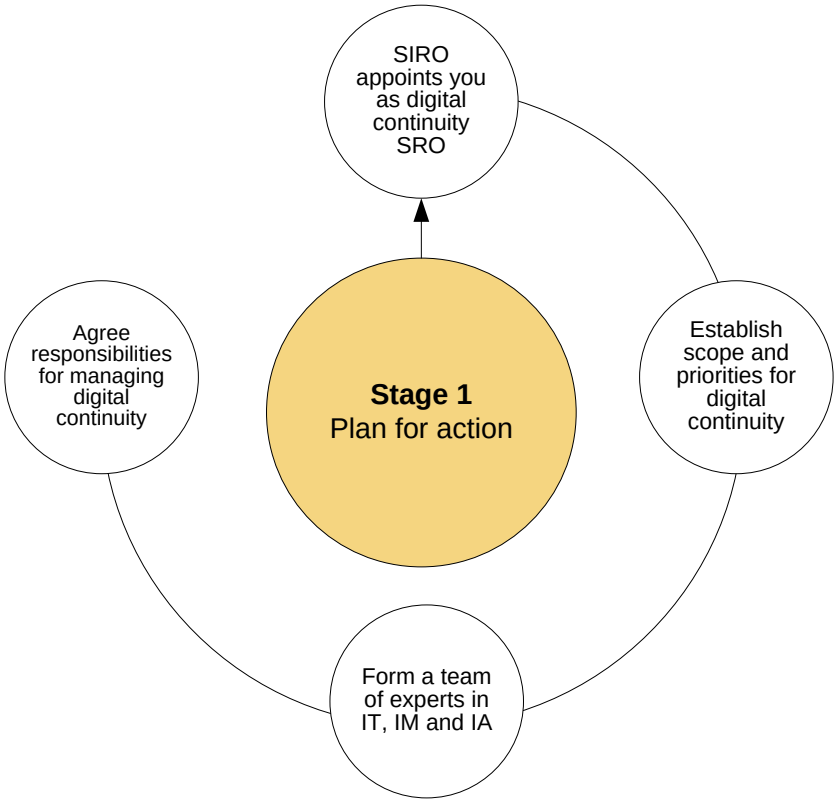

Figure 1: plan for action

To manage your digital continuity effectively, you need buy-in from individuals across your organisation. Senior managers need a good understanding of the benefits and risks to continuity in order to champion appropriate governance and action at all levels in the organisation.

Individuals from several disciplines, including information technology (IT), information assurance (IA), information management (IM) professionals and change management, need to collaborate to help to manage digital continuity. If you are managing digital continuity across your organisation, it is important for someone to lead this group of individuals and drive the process forward – this is your role, as the appointed Senior Responsible Officer (SRO).

You are responsible for overseeing and promoting digital continuity management in your organisation. You will need to assess where you can build on or amend existing work practices, policies and systems to ensure that all teams are operating in a way that can deliver digital continuity. You should also allocate the resources you need to embed this as part of business as usual operation and change management.

You ensure that the right systems and structures are in place, that risks are managed and that the business requirement for digital continuity is expressed in any relevant strategies and plans. You have a clear route for elevating issues to board level as necessary.

Actions to take

The following actions will kick-start your organisation's approach to digital continuity management:

1. **Your Chief Executive Officer (CEO) appoints you as a SRO to take action on digital continuity.** It could be that your CEO is already well aware of the risks to digital continuity and has given you a clear indication of what your role is and your drivers for managing digital continuity, or it could be that you have to be more proactive and get to grips with the role yourself. If your CEO has not yet appointed a SRO for digital continuity, you should highlight to them why it is important for them to do so, help raise awareness of the need to manage digital continuity in your organisation, and start to take action. Whatever point you come to the process, help is at hand in this guide to managing digital continuity.

2. **Establish scope and priorities for digital continuity.** How you need to use your information will depend on your department or organisation's needs.

   Considering what brought you to this point will help you to define your priorities and starting point. You need to plan the scope and scale of your approach – you do not have to begin by managing digital continuity for the entire organisation; you may want to **start small** and begin by assessing digital continuity management for a particular project or business unit. For instance, if you need to reduce costs in the IT department, you should begin by speaking to the Head of IT. Whatever the scale of the project, you can still use this four-stage process and tailor your individual objectives accordingly.

3. **Form a team of experts in IT, IM, IA and change management to help manage continuity.** You will need expertise from other teams to help you to understand how your business uses its information and whether or not your information and IT management support that use. You must consider how digital continuity fits in with your organisation's strategic vision for IM, IT, IA and change management and into relevant policies, projects and business planning. Best practice would be to form a multi-disciplinary team to manage digital continuity. The key is for these individuals to communicate, one way or another, on a regular basis.

4. **Ensure that all relevant individuals across the organisation, including managers in the IT, IM, IA and business change functions, understand digital continuity and their roles in exploring the issues.** Our introductory guidance Understanding Digital Continuity should help key stakeholders to understand issues and risks. We are also producing guidance on the individual roles and responsibilities you should assign to manage digital continuity to help individuals to understand their specific responsibilities.

What next?

Once you have established your scope and priorities and gained collaboration and across the organisation, the next step is for you to follow Stage 2 of our guidance, *Define your digital continuity requirements*.