The National Archives

Managing Digital Continuity

Stage 2: Define your digital continuity requirements

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 2

This guidance is to help you to define your requirements for digital continuity. This involves understanding your information assets, their business value and the nature of the technical and information environment that supports them.

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 1: Plan for action*, we provided you with help to get started in managing digital continuity. That is, establishing your objectives: who you need to work with, and how to go about managing digital continuity across the organisation. Now it's time to analyse what information you have that you need to protect for the future, and how you need to use it.

This guidance deals with Stage 2 of this process, which comprises the following actions:

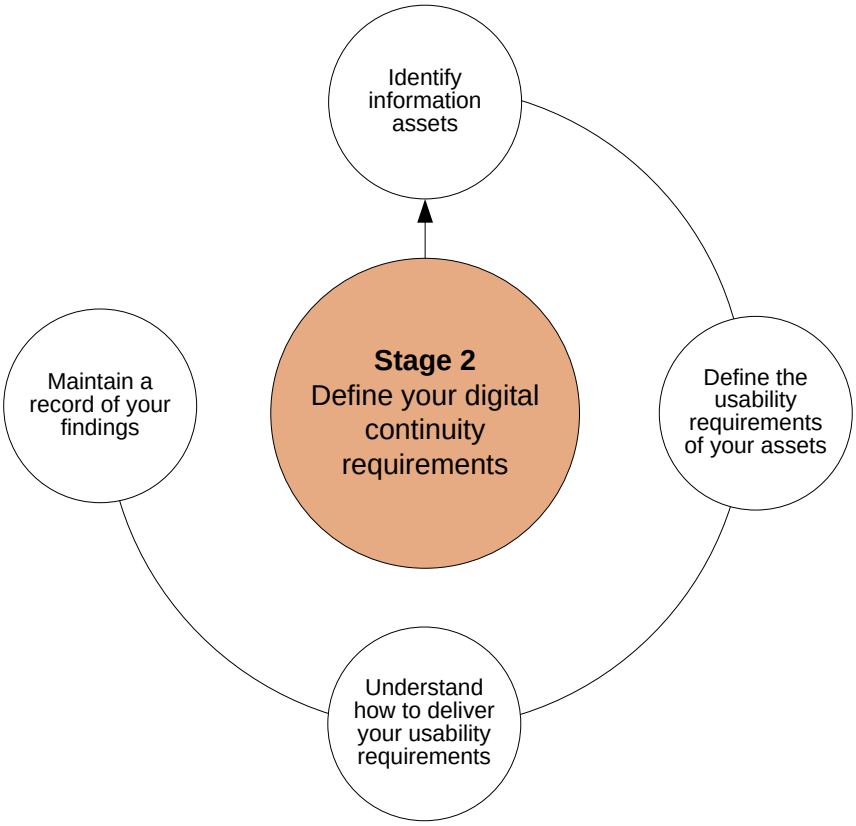

Figure 1: define your digital continuity requirements

Defining your digital continuity requirements means establishing what digital information you have, what you need to keep and how you will need to use it, over time and through change.

Once you understand how your business needs to use information, you can ensure that your technical environment and the way you manage your information continue to support this use in the most efficient way. It should also highlight where savings can be made by eliminating unnecessary information or technology.

To do this, you must first understand what information assets you have. An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Once you have identified your information assets, you must determine how you need to use each of them – these are your business needs. This covers everything from how you find it, through how you access it to what you do with it.

The digital continuity of your information is maintained when your business requirements, technical environment and information assets support one another, so to ensure continuity you will need to map the relationships between these elements, identifying shortfalls in support, or unrequired capability.

These elements can easily change and fall out of sync with one another if these changes are not effectively managed. You could be left with information assets you can't use, or technology supporting information in a way that doesn't meet your needs. See Figure 2 below.

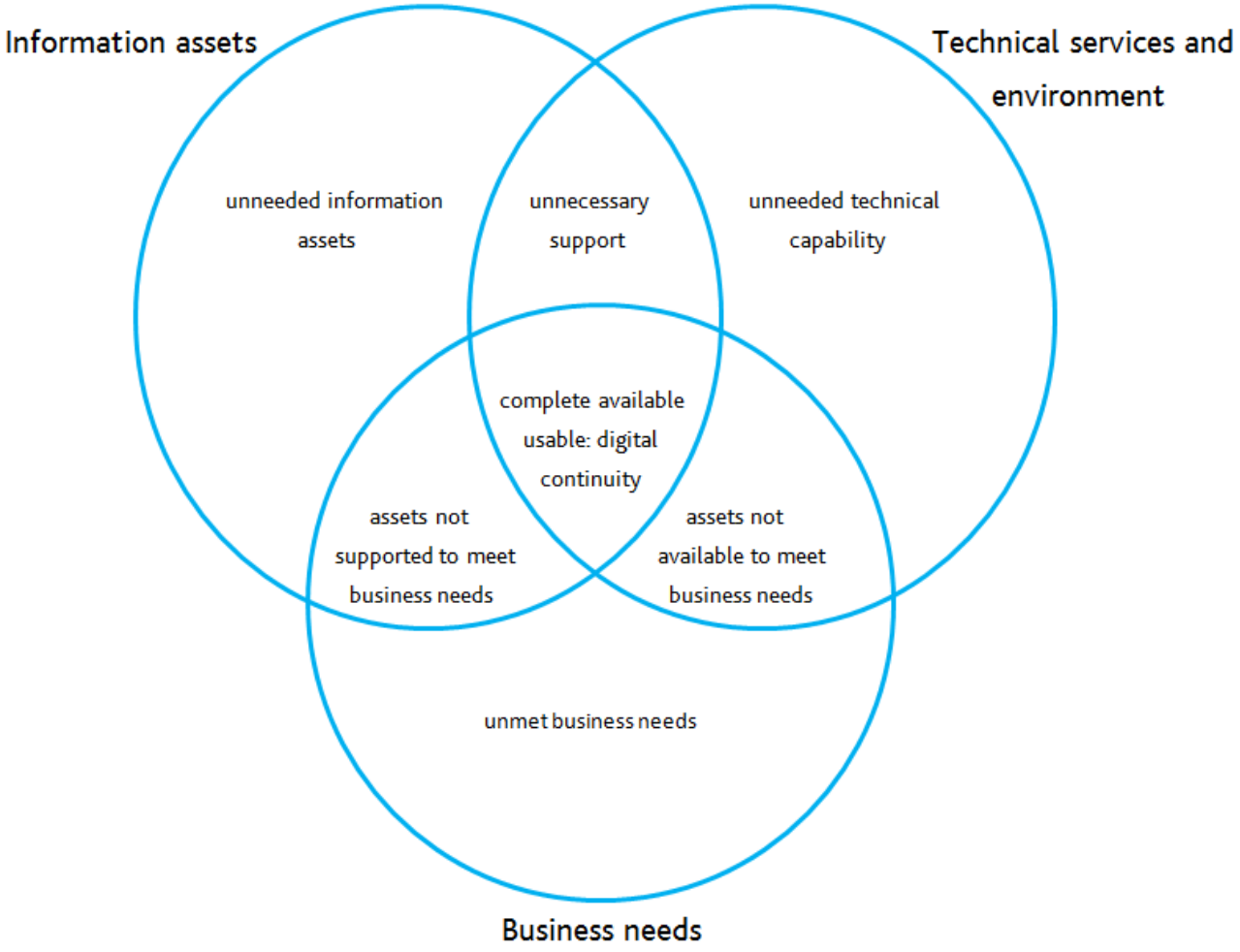

Figure 2: ensuring Digital Continuity

Action to take

Here are some high-level actions you need to take. For more detail on what to do in practice, read our guidance *Identifying Information Assets and Business Requirements* and *Mapping the Technical Dependencies of Information Assets*.

1. **Identify your information assets**

    - Identify what information assets you have – categorise your information from the perspective of its content and business use, not in terms of the Information Technology (IT) system that holds it

- When you identify your assets, you should consider the level of granularity that is required to meet your objectives. An information asset is defined at a level of detail that allows its constituent parts to be managed usefully as a single unit
- Be sure to address all forms of information generated by your organisation, including that which exists primarily on web platforms, and not only personal/sensitive data but all the information a business needs

2. **Define the usability requirements of your assets**

- Identify how you will find your information; who can access the information and how; what you need to be able to do with the information; what you need to be able to understand about your information; to what extent you need to trust that your information is what it claims to be
- Consider your future usability requirements

3. **Understand how to deliver your usability requirements**

You need to understand how to deliver these usability requirements – the level of completeness and availability required from your assets. The process of mapping your information assets and business requirements to their technical environment and information management policies and processes will help you to do this.

- **Map your information assets and business requirements to your technical environment.** You will need to undertake a technical mapping exercise to establish your technical dependencies. This will tell you the technology components you rely upon to help ensure your information is complete and available for you to use as needed. Outputs from enterprise architecture tools, a configuration management system or other technology management tools you already have in place may be able to help you with this. You will need to understand:
    - the software applications you use (both desktop and enterprise applications)
    - the hardware platforms and infrastructure
    - the skills and expertise you rely on to manage the technology
    - planned changes to the technical environment and its expected end of life

- **Ensure you have processes in place and have defined ownership responsibilities to keep information about your technical environment updated and reviewed regularly for completeness.**

4. **Maintain a record of your findings.** You need to compile a comprehensive mechanism for mapping your information assets, usability requirements and technical and information environment dependencies. You may have existing systems which can be exploited, for example an *Information Asset Register* (IAR), hardware or software asset registers, or configuration management databases (CMDBs). You need to ensure you can cross-reference various sources of information in the way you need to. You must ensure you keep this record up to date to retain digital continuity.

Next steps

Once you have defined your information usability requirements, the next step is for you to follow Stage 3 of our guidance, Assess and manage risks to digital continuity.