The National Archives

Managing 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.

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.

What constitutes 'usable' will be different depending on your business' needs for each piece of information. Understanding your usability requirements is a key part of managing your digital continuity. In practical terms, your information is usable if you can find it, open it, work with it, understand it and trust it. You need to establish how to keep your information complete and available in order to meet your usability requirements.

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 provides a high level guide to the steps you can take to manage digital continuity. It assumes a basic understanding of what digital continuity means, as outlined in our *Understanding Digital Continuity* document.

Following our guidance will enable you to:

- establish your scope and priorities for digital continuity
- establish responsibilities and resource commitments and allocate roles for taking action to ensure digital continuity
- define your digital continuity requirements
- prepare to assess risks to digital continuity
- prepare to embed digital continuity in your information management, IT strategy and environment, and change management.

The National Archives has developed a service for government, and the wider public sector, that will help you to assess your specific risks to digital continuity and to plan and take action. This includes a suite of guidance which gives you more detail about the four stages outlined in this document.

1.2 Who is this guidance for?

This guidance is primarily aimed at the person who has been given overall responsibility for ensuring digital continuity over time and through change – the Senior Responsible Owner (SRO) for digital continuity. This responsibility includes driving forward actions relating to digital continuity and establishing resources necessary to deliver digital continuity and identify risks. The document will also therefore be useful to departments and SROs so they can better understand the responsibilities they must assign.

This guidance will also be of use for staff with responsibility in managing digital continuity. The specific roles may vary, but examples include:

Information assurance:

- Risk managers
- Information Assurance (IA) programme managers and other IA professionals
- Information Asset Owners (IAOs)

Information management:

- Heads of Knowledge and Information Management
- Information managers – Information Management (IM) professionals and Department Records Officers (DROs)

Information technology:

- Chief Information Officers (CIOs) and Chief Technology Officers (CTOs)
- Information architects/Information Technology (IT) strategists
- IT service managers/suppliers
- Procurement managers and commercial contract managers

Change management:

- Business change managers, project and programme managers

2 Managing digital continuity

This guidance outlines a four-stage process your organisation can follow in order to manage digital continuity coherently and effectively.

This model is flexible – you can enter at any stage and you may find that you don't need to undertake every action – it will very much depend on your business needs. You can also adjust the scope to cover either your whole organisation, just an individual business unit, or if you are managing a specific change. The stages laid out here should give you a clear idea of the types of action you might take.

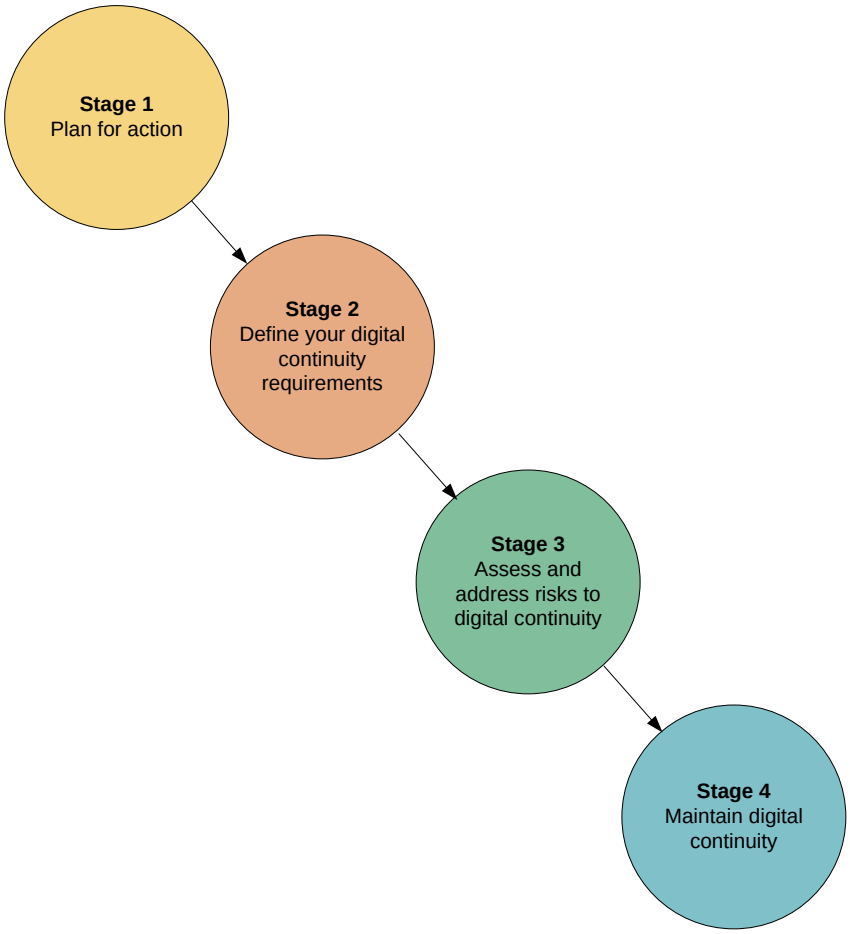

Figure 1: managing digital continuity

2.1 Stage 1: Plan for action

This section of the guidance will help you establish your objectives, who you need to work with, and how to manage digital continuity across the organisation.

Stage 1 of this process comprises the following actions:

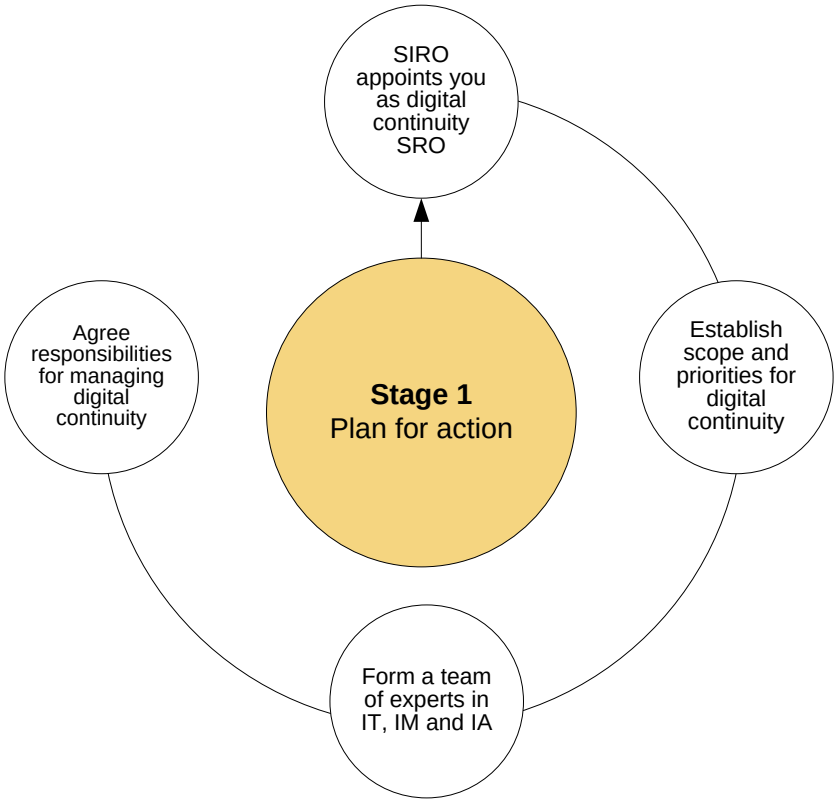

Figure 2: plan for action

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 IT, IM, information assurance (IA) and change management professionals 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 responsibility, as the appointed 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 need to 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. **Appointment as SRO to take responsibility for digital continuity.** It could be that your CEO or Senior/Executive Team is already well aware of the risks to digital continuity and has given you a clear indication of what your responsibilities are and your drivers for managing digital continuity, or it could be that you have to be more proactive and get to grips with the responsibilities 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 responsibilities in exploring the issues**. Our introductory guidance Understanding Digital Continuity should help key stakeholders to understand issues and risks.

2.2 Stage 2: Define your digital continuity requirements

This section of the guidance guides you through defining 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.

Stage 2 of this process comprises the following actions:

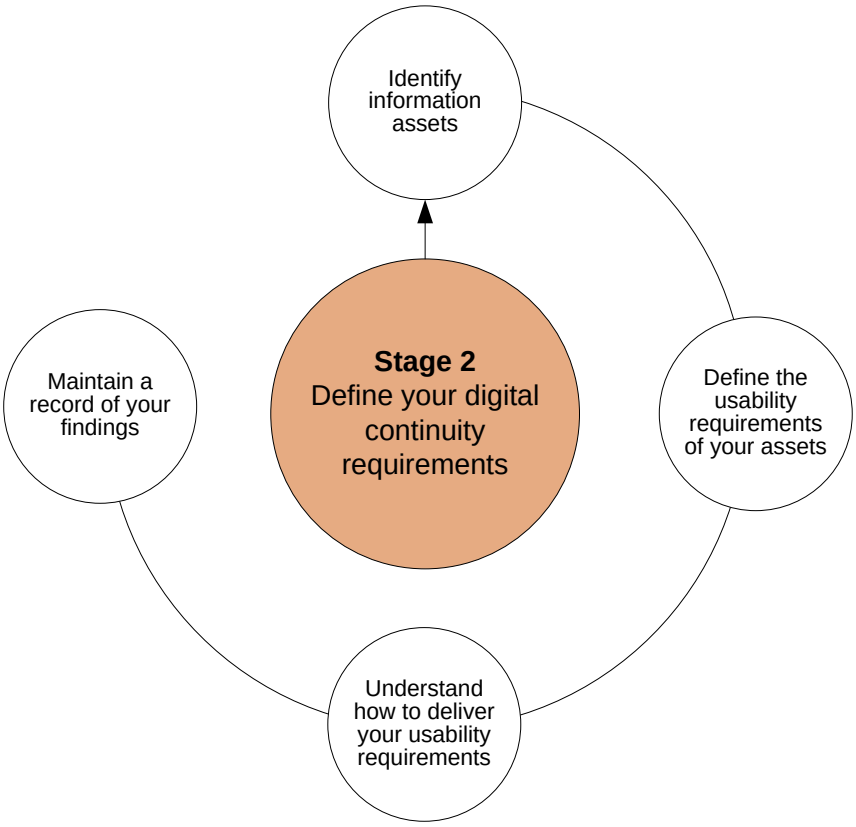

Figure 3: define your digital continuity requirements

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 identify and 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.

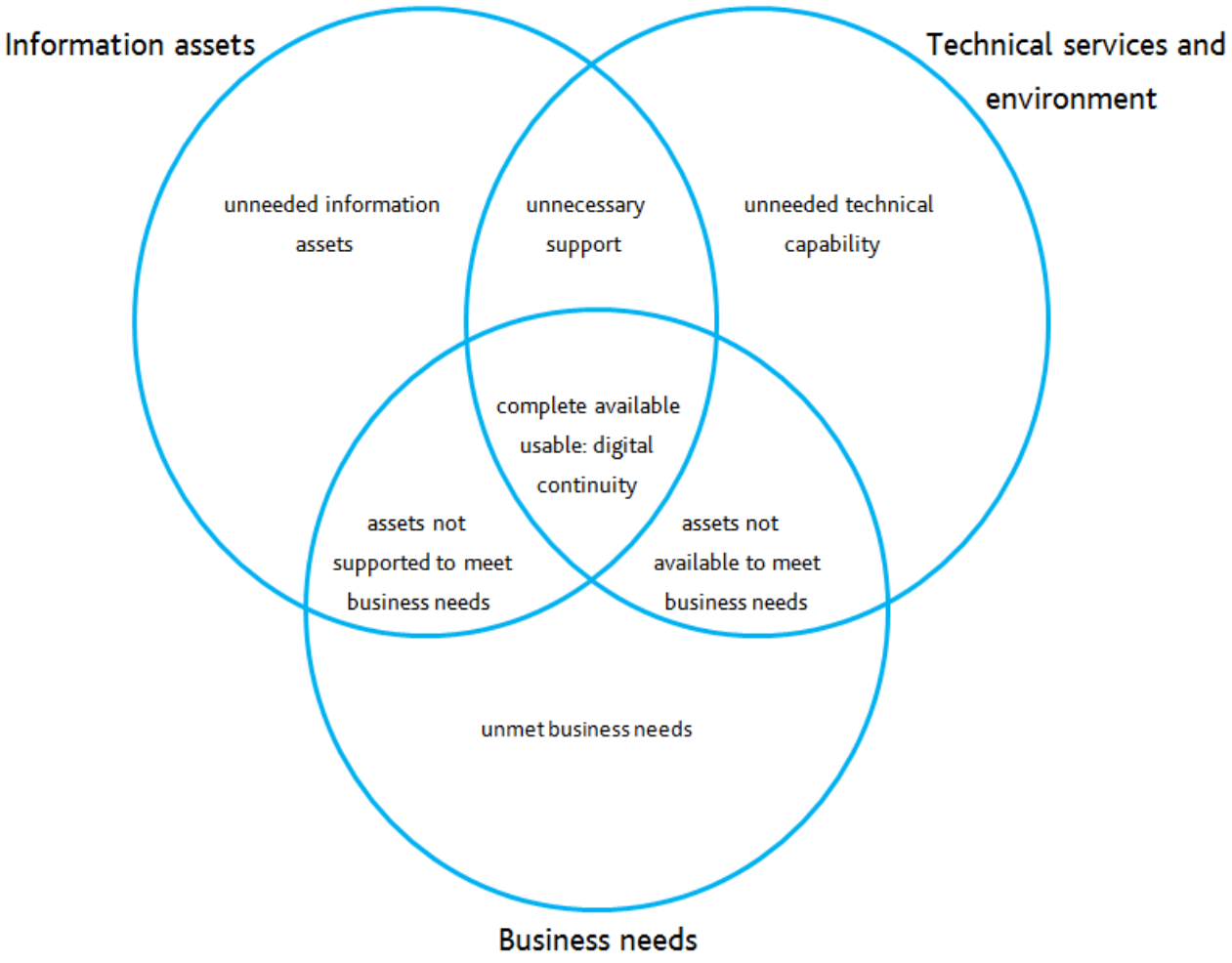

Figure 4: ensuring digital continuity

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.

Actions to take

Here are some high-level actions you need to take. For more detail on what to do in practice, read our guidance on *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 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 will you 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.

2.3 Stage 3: Assess and manage risks to digital continuity

This section of the guidance will help you to manage the risk of losing digital continuity by setting out appropriate governance and risk management structures, assigning responsibility for the management of risk to digital continuity, and assessing your current level of risk.

Stage 3 of this process comprises the following actions:

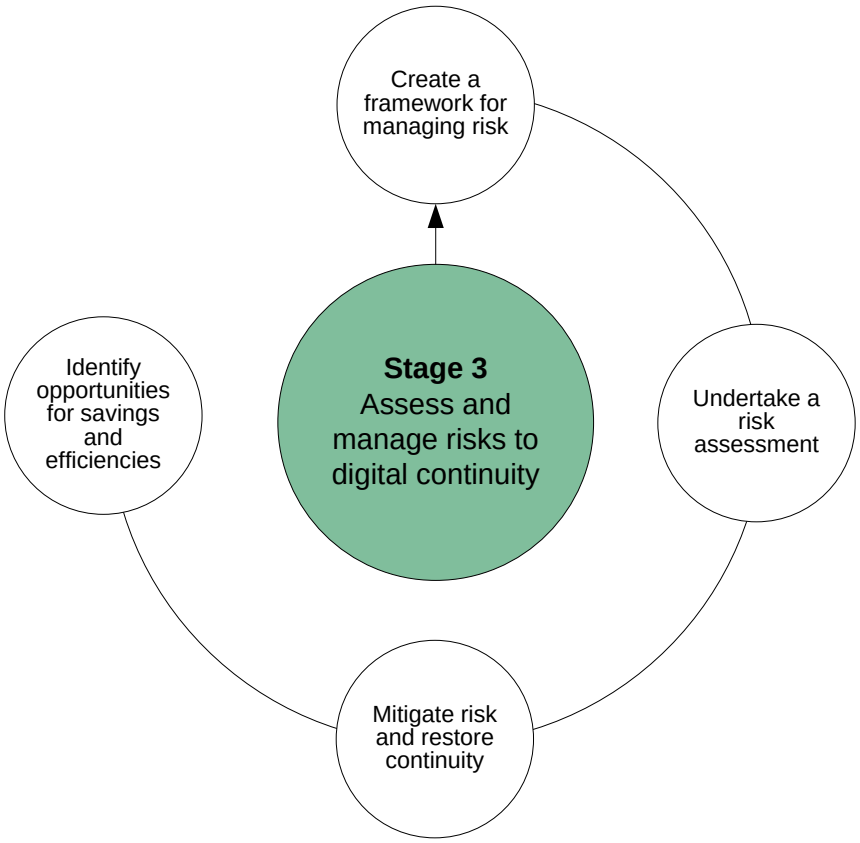

Figure 5: asses and manage risks to digital continuity

Undertaking a comprehensive digital continuity risk assessment for your organisation will enable you to:

- assess the risk you face
- prioritise key areas of concern
- plan and take action to mitigate your risks

You should manage risks to digital continuity in line with your general information risk management procedures and (for government departments) the CESG Information Assurance Maturity Model (IAMM). Risks to digital continuity should be recognised at an organisational level, and at a more granular level in the areas of information management, IT management, information assurance and business change.

Larger organisations may wish to take a phased approach to risk assessment, tackling priority areas first.

Actions to take

1. **Ensure that there is a clear framework for managing risk to digital continuity within your organisation (though allocation of responsibilities to specific roles may vary between organisations):**

    - Ensure you understand the need to manage risks to digital continuity as you would any other information risk
    - Ensure your organisational risk appetite is informed by a good understanding of the business value of your information and the consequences of losing it
    - Identify the specific responsibilities of the IM, IT and IA teams for managing risks to digital continuity
    - Ensure each of your information assets has an Information Asset Owner with responsibility for managing risks to their information asset

2. **Undertake a digital continuity risk assessment for your organisation**

    - Arrange an initial risk assessment and action planning exercise
    - Undertake an assessment of risks to digital continuity, identifying and prioritising key risks and any existing issues arising from the assessment
    - Profile the file formats you are using and creating to understand which are at risk of obsolescence and how soon. The National Archives has developed a file identification tool (DROID) to assist you by identifying file formats and versions. You can then use the information available in the DROID: user guide to help you understand and manage the risks to your digital information

- Ensure outputs are reflected in information risk registers

3. Mitigate risk and restore continuity

- Develop an action plan to address these risks to be taken forward by your digital continuity project team, with timescales and resources as appropriate
- Reduce your risk through taking action to decrease either the probability or the impact of the risk. For example, placing information into the public domain would reduce the operational impact of a loss of continuity, since the information would be recoverable from an external source (such as an internet archive)
- If you have identified failures, you may need to consider restoring continuity for any specific issues you've identified. However, it may not be cost-effective (or even possible) to restore continuity in this situation. It's most important to learn from what happened to help you mitigate the risk that it will happen again

4. Identify opportunities for savings and efficiencies

By understanding your requirements and assessing your risks, you may also identify opportunities for cost savings and efficiencies (see also Stage 2, Figure 4), including:

- disposing of any information assets that you no longer need for business requirements, reducing storage and resource costs
- streamlining your technical environment and increasing IT efficiency, for instance by downgrading technology, saving money on expensive systems or unnecessary functionality
- moving information assets to cheaper, more efficient and effective storage

2.4 Stage 4: Maintain digital continuity

This section 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.

Stage 4 of this process comprises the following actions:

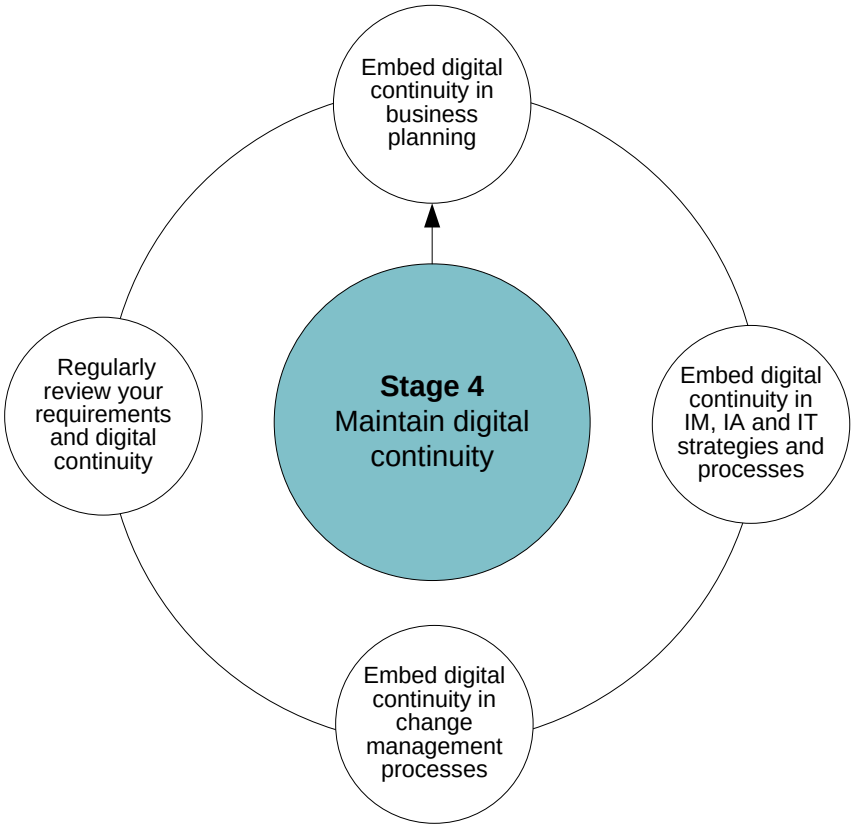

Figure 6: maintain digital continuity

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 IM and 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 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 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

3 Roles and responsibilities

This section of the guidance identifies how different roles across the organisation have specific responsibilities for managing digital continuity.

Every organisation is different and roles, responsibilities and job titles may vary – so you may assign responsibilities differently in practice. But this section should give you a generic overview of who needs to do what.

Roles may be grouped broadly as:

- Governance, including CEOs and Non-Executive Directors
- Senior management, including Information Asset Owners
- Specialists, including individuals in information management, IT, information assurance, business change managers
- All other staff

Specific roles in central government may include the following:

Role	Digital continuity responsibility
Chief Executive Officer (CEO), or Executive/Senior Team	Appoints the SRO and ensures that risk to digital continuity is adequately identified and mitigated, as an integral part of the departmental information assurance and risk management strategy
Senior Responsibility Owner (SRO)	Owns the business objective of digital continuity, is the operational lead on ensuring digital continuity is managed and embedded across the organisation
Chief Information Officer (CIO)	Owns and champions the business outcomes and benefits of ensuring the continuity of information assets
Information Assurance (IA) Programme managers and other IA professionals	Ensures that digital continuity is addressed as part of the spectrum of information assurance and risk management measures within the organisation
Risk managers	Ensure that any risks to digital continuity identified by digital continuity risk assessment processes are properly managed through their organisation's risk

	management framework
Head of Knowledge and Information Management (KIM)	Leads work on defining what business use the organisation needs to achieve from its information assets and over what timescale Also ensures information usability requirements are articulated and integrated into relevant Information Management/Record Management strategies and policies, and business change processes
Information Managers (IM professionals and Department Records Officers (DROs))	Work with head of KIM to identify risks to digital continuity and issues for the organisation
Information Asset Owners	Understand what information assets they are responsible for, the usability needed from those assets and the risks to the continuity of the assets Maintain information about those assets in an IAR and ensure that processes are in place to support the digital continuity of the assets
Chief Technology Officers (CTOs)	Ensure the organisation's technical environment enables the continuity of information assets in line with the business requirement, over time and through change
Enterprise Architects / IT strategists	Ensure that enterprise architecture and/or IT strategies properly account for the ongoing business need to use information over time and through change. Maintain a close dialogue with other colleagues from IM, IA and business change who are involved in digital continuity
IT service managers	Ensure technology is delivered and maintained to enable continuity of information assets in line with the business requirement Ensure that IT service change management processes take account of the impact on the digital continuity of information assets
Procurement managers, Commercial/contract managers	Ensure that appropriate responsibility for identifying and managing continuity issues is clearly defined in

	supplier contracts, including referring to an IAR, with defined service outcomes describing the usability required for each information asset
Business Change Managers, Project and Programme managers	Ensure that digital continuity is appropriately taken into account in any business change process
Heads of e-Comms	Ensures business and continuity requirements are articulated and integrated into relevant IM and IT strategies and policies, and business and technological change processes Has a key responsibility in the operational work to ensure digital continuity is addressed on an ongoing basis by the organisation

4 Ensuring confidence in your continuity

Digital continuity is the ability to use your digital information in the way you need, for as long as you need. You must understand your business requirements and be aware of the risks to the continuity of your information to ensure you retain its usability. If you fail, you will be unable to use your information in the way you want, when you want.

4.1 How do I know if I have continuity?

If you are successful in managing your digital continuity, your information will be complete, available and therefore usable in the way you need. In other words:

- you can find the information you need
- you can open the information you need
- you can use or work with your information in the way you need
- you understand what your information is and what it's about
- you trust your information is what it says it is

4.2 Key measures

To ensure you are managing information as a valuable asset, you need to embed digital continuity in day-to-day business across the organisation. This section provides you with a checklist of processes and ways of working you should have in place to ensure you are managing your digital information effectively.

Stage 1:

- A SRO has been appointed by the CEO or Executive/Senior Team
- The scope and priorities for digital continuity have been set
- You have established a group of individuals from across disciplines, including managers in the IT, IM, IA and business change functions, to help manage digital continuity
- You have ensured that all relevant individuals across the organisation understand digital continuity and their roles in exploring the issues

Stage 2:

- You have identified your information assets
- You have defined their usability requirements
- You have mapped these assets and their requirements to their technical environment

Stage 3:

- You include information management risks in existing risk processes
- You have undertaken a risk assessment
- You have made an action plan to mitigate risk, restore continuity and realise savings and efficiencies
- You have followed that action plan
- You feed into existing reporting structures such as the IAMM and The National Archives' Information Management Assessments (IMAs)

Stage 4:

- You have embedded digital continuity requirements into business planning and service delivery processes and related policies
- You include information as part of your change management policies and procedures
- You test business critical information before and after change to ensure you can still use it as you need to