The National Archives

Understanding 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.

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 information because you haven't managed your digital continuity properly, the consequences can be as serious as those of any other information loss.

Managing digital continuity is essential if you are to protect the digital information you depend on to do business. Losing your digital continuity could have serious consequences (see Appendix).

1.1 What is the purpose of this guidance?

This piece of guidance is a high level introduction to digital continuity – what it is, why it's important and why it's relevant to you and your organisation. It also contains an overview of how you can better manage it, and what your next steps could be.

It 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.

1.2 Who is this guidance for?

This guidance is aimed at anyone who wants to know more about digital information management and digital continuity. Whether you have been given a specific role to fulfil, or if you are just reading to improve your knowledge, this is a good starting point.

2 What is digital continuity?

Imagine if:

- you couldn't find information for a public inquiry
- you couldn't claim emergency financial assistance because your financial data is buried in out-of-date software
- you couldn't pay pensions because you lost the metadata connecting people to the contributions they'd made
- you had to spend time and money recreating expensive multimedia data that you couldn't work with because it was in an obsolescent format
- you needed records of decisions for legal compliance, but had no way of telling if you were looking at the final version of documents

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.

Information is at the heart of good government, but without due care and consideration the digital information on which government depends is less likely to survive and remain usable than paper records.

Your digital continuity is most at risk during changes in your organisation, management processes and technology. You need to manage your information carefully over time and through such changes to maintain the usability you need.

Digital information is more vulnerable than paper for a number of reasons, including:

- There's more of it and it's created in a diverse range of formats; opening and using it depends on hardware and software that can become unsupported
- It can be stored in a variety of places, making it harder to find
- It is easy to lose essential metadata and context required to understand the information when it is moved between organisations and systems
- Multiple versions of the same information can exist, making it difficult to determine which version is most accurate or up to date
- Essential audit data that tells us what has happened to the information, who accessed or changed it and when, can be lost – making it difficult to trust the information

Understanding how you need to use your information is a key part of managing your digital continuity. For more information on information assets and usability requirements see our guidance on *Identifying Information Assets and Business Requirements*. What constitutes 'usable' will be different depending on your business' needs, but in practical terms, your information is usable if you can:

- **find** it when you need it
- **open** it as you need it
- **work with** it in the way you need to
- **understand** what it is and what it is about
- **trust** that it is what it says it is

You need to establish what your information's usability requirements are, based on the business outcomes it needs to fulfil.

This understanding will enable you to put in place and manage the processes and technologies required to keep the information complete and available so that it meets the usability requirements.

USABLE = AVAILABLE + COMPLETE

Usable: your information meets your requirements for how you want to use your information.

Available: you can find what you need and you have the technology to open it and work with it in the way you need.

Complete: everything you need to use, understand and trust the information is present, including the content, context and all the necessary metadata.

2.1 Why does it matter?

Managing digital continuity is essential if you are to protect the digital information you depend on to do business. This enables you to operate accountably, legally, effectively and efficiently. It helps you to protect your reputation, make informed decisions, reduce costs, and deliver better public services. Understanding the principles of digital continuity and the serious consequences of losing it will prepare you for managing it in your organisation.

The process of managing digital continuity (see section 4) starts with understanding what value your information has and how it is used to deliver business needs. You then need to ensure that your technology and information management processes support your information assets in meeting these business needs. If they don't, you're at risk of losing the ability to **find**, **open**, **understand**, **trust** and **work with** your information, which could have considerable impact on your ability to do business. The Appendix contains real-life case studies, which illustrate what can happen when you lose your digital continuity.

The process of understanding what information you have, how you need to use it and how to support it for as long as you need it may also reveal information or technology you no longer require. You can then make savings by simplifying your information and streamlining your technologies, helping you to reduce data volumes and dispose of unnecessary Information Technology (IT) systems. Other benefits of managing digital continuity are being able to work more efficiently and effectively, and supporting your information assurance and security.

2.2 Digital continuity in context

> 'Authorities should know what records they hold and where they are, and should ensure that they remain usable for as long as they are required'
>
> Code of Practice on the Management of Records under section 46 of the Freedom of Information Act

Without active management of digital continuity, there is a risk that over time that organisation will be unable to find and use the digital information they need to do business, to deliver public services, or to maintain accountability.

Managing the digital continuity of your information will help you to meet your legal obligations, deliver improved information assurance, and support the transparency of your organisation.

2.2.1 Legal requirements

You have a duty to manage your digital information appropriately, in line with legal requirements and best practice guidelines. There could be repercussions if reliable, verifiable information is not made available to the public or for an inquiry as and when it is required.

Your responsibility to look after information may include:

- Managing information about employees and members of the general public, which is covered by the Data Protection Act

- Statutory responsibilities relating to specific types of records, such as the Public Record Act 1958
- Complying with the Freedom of Information Act 2000 (according to the revised FOI section 46 Code of Practice, which sets out recommended good practice for managing records and includes requirements for being able to use your records)

2.2.2 Information assurance

Loss of digital continuity is an information risk like any other, which organisations across the public sector need to manage as part of their information assurance and information risk management approaches. Management of digital continuity is part of the Information Assurance Maturity Model and Assessment Framework and those accountable for managing information risk, such as Chief Executive Officer (CEO) or Executive Team and Information Asset Owners (IAOs) need to understand that maintaining digital continuity is core to their role.

2.2.3 Transparency agenda

Managing digital continuity can help you meet your obligations under government policies on transparency and the public's 'right to data'. Having confidence that your digital information is complete, has context and is trustworthy is an essential first step. In addition, managing your information in open and standardised formats mitigates many continuity risks and will make it easier to find, share and repurpose.

3 What does digital continuity look like?

The digital continuity of your information is maintained when your technology and information management processes support your information assets in meeting your business requirements both now, and in the future. This is when:

- you know what information you have, what it is about and where it is
- you understand how you want to use it, now and in the future
- your technology and information management process enables you to use your information, and is agile enough to cope with your changing requirements

This is illustrated in the diagram below, which shows how digital continuity is achieved when your technology supports the business use you need from your information assets.

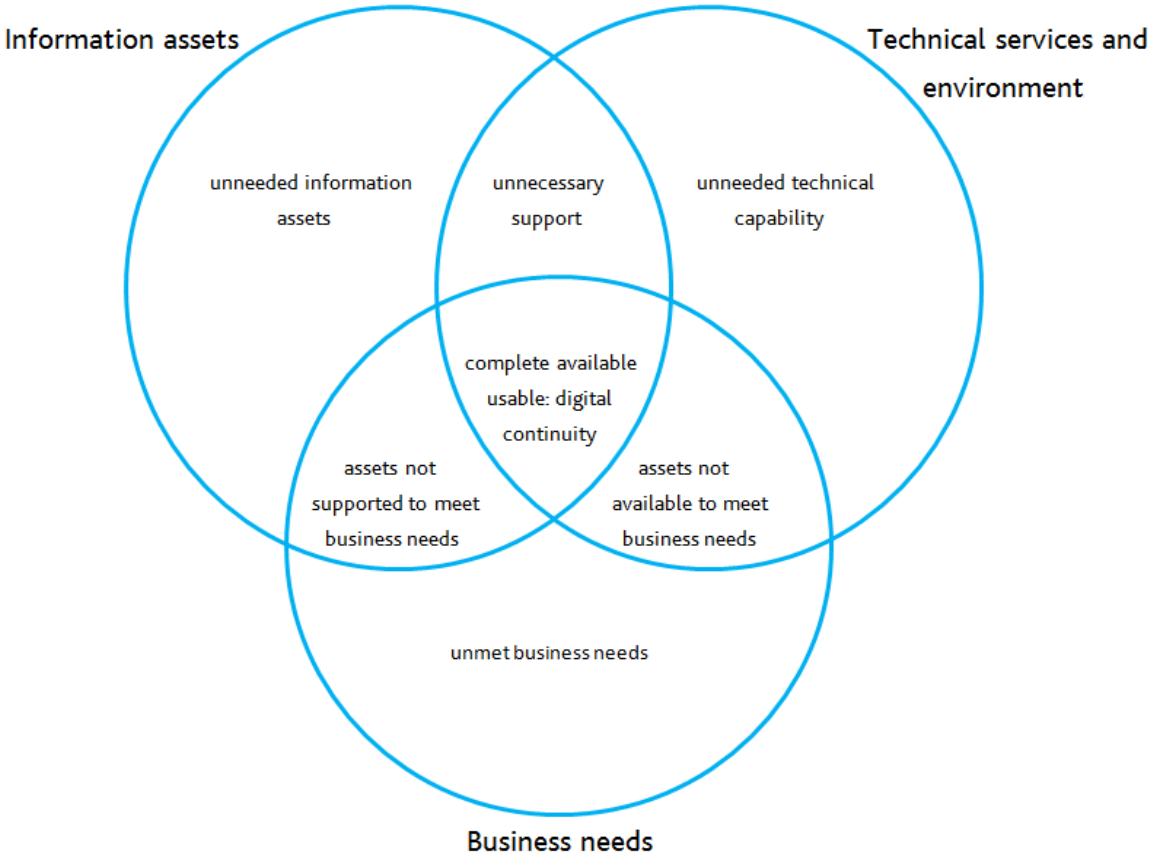

Figure 1: ensuring digital continuity

Once you understand the usability requirements for your information, and the technology and processes you are dependent on to provide this use, you can effectively identify when change is likely to impact on your information, and manage it to ensure that your digital continuity is maintained.

4 Managing the risks that change brings

Managing change is key to managing digital continuity. As shown in Figure 1 above, digital continuity is about the alignment between your information, your usability requirements and the complex technological environment which supports it. Changes to any of these elements, even seemingly minor ones, could have a dramatic impact on your ability to use your digital information. Managing change means identifying when your information might be affected by a change, undertaking impact assessments to understand where there might be risks to your digital continuity, and putting in place effective plans to ensure that you keep your information usable through the change.

If 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. At best, this creates inefficiencies. At worst, it can result in the loss of the information you need.

It's not only immediate changes that you need to think about, there is also the risk that you are unprepared for change in the future. You should consider how you will want to use information, for instance in five years' time – are your business needs likely to change? Have you planned the lifecycle of your hardware and software so that you know when change is likely and can plan your strategies for maintaining digital continuity in advance? You should also have succession plans in place, so you have some contingency if staff critical to managing your information and IT leave the organisation.

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. It means ensuring that digital continuity is reflected in your business plans and strategies, policies and risk and change management processes.

Failure to manage your digital continuity through change can mean:

- information ownership becomes unclear, with information not appropriately incorporated into information governance and management structures
- information risks are missed or unmanaged if ownership and supporting information risk management processes change
- information is not disposed of appropriately, with increased liability in terms of management and compliance
- information is not migrated to new technologies effectively, with loss of critical content, metadata, context, audit data meaning that you can't use the information appropriately upon migration

- information is trapped in ageing, legacy IT systems, with restricted access, limited functionality and increased support costs
- information becomes locked in a format that can't be opened or used by the technology that's available to you, or that technology does not provide you with the functionality you need
- information is no longer understood by the organisation as it loses staff who manage the information, understand its context, or have scarce expertise in the supporting technology
- information is not trusted, if crucial audit data, logs, versions and contextual information are not maintained

There are three key types of change you need to consider:

4.1 Business or organisational change

If your business goes through a transition, for example a Machinery of Government (MoG) change, or needs to respond to new opportunities and challenges, the way you need to use information may also change.

You will have digital continuity issues if your information assets, information management and IT systems do not support the new way your business needs to use your information. Staff changes can result in a loss of vital understanding of context or expertise in operating technology.

4.2 Technological change

Changes to your IT environment can impact on digital continuity. For example, during transfer of information to new formats or systems you could change or lose the essential metadata, context and audit data you need to keep the information complete, or find that you don't have the technology you need to work with it in the way you need to.

As digital information often has a lifecycle that it much longer than the technology that supports it, changes to technology need to be carefully managed to ensure you can still use your information. Technologies can become unavailable and obsolete, for instance if formats or applications are no longer supported or are upgraded, digital information can become trapped in ageing legacy IT systems. In the worst case scenario, you may find your information becomes locked in software or hardware formats that you no longer have the technology to open or use.

4.3 Information asset and management change

Changes to the information assets themselves, and the management environment for that information, can also put your digital continuity at risk. For example, if you change the way you structure your information and file stores, change your metadata policies and processes or change the context of the information, you may find you can no longer find it when you need to, or understand and interpret the information correctly.

5 Next steps

Ensuring continuity requires ongoing planning, action and collaboration between those responsible for information management, IT, business change and information assurance. It cannot be managed successfully by any one of these disciplines acting alone.

You should start by finding out whether your organisation is already managing its digital continuity. If it is, find out who is in charge of it in your organisation and see how you can help. If no one is yet assigned to managing digital continuity in your organisation, why not take charge? You could begin by speaking to your CEO or Executive Team, who will take this forward and should assign a Senior Responsible Owner (SRO) for managing digital continuity.

If you have been appointed a SRO for digital continuity, your next step is to read our guidance *Managing Digital Continuity,* which outlines a four-stage process for managing digital continuity in your organisation.

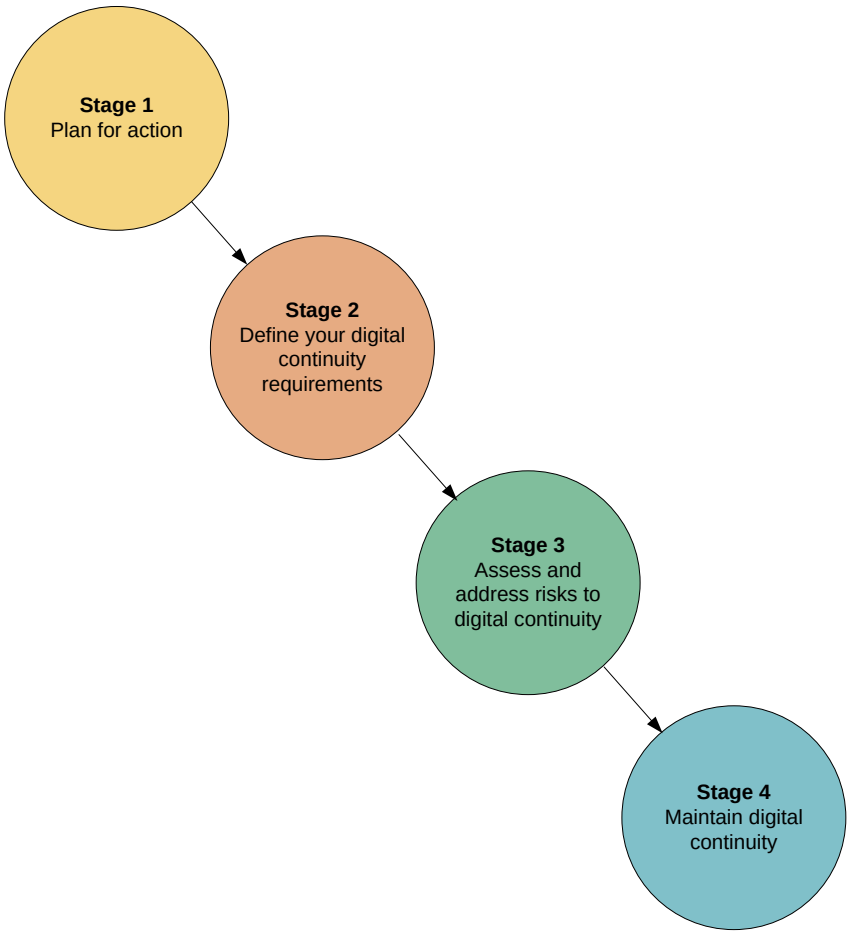

Figure 2: managing digital continuity

5.1 Guidance

The National Archives offers a suite of guidance to help you manage digital continuity in your organisation. As mentioned above, Managing Digital Continuity is a useful place to start, as it provides a guide to our four-stage process.

If your organisation is going through any change that may affect digital continuity, there is also a subset of our guidance package designed to support this – *Change Management for Digital Continuity SROs* gives an overview of how to take care of your information through change and links to practical how-to guides for specific types of change.

5.2 Risk assessment

The Information Management Assessment team at The National Archives have built a self-assessment tool, allowing you to assess risks to the continuity of your information. This assessment falls within Stage 3 of the managing digital continuity process, but can also be performed in isolation.

5.3 Digital Continuity Framework

To support your organisation's management of digital continuity, there is a range of services and solutions available on the Crown Commercial Service website for your organisation to procure. The services available provide expertise in specific areas of information management and IT. They cover not only advice and guidance on new systems and processes, but also focus on improving the use of what is already in place to achieve the best value. The solutions available cover technology to improve particular areas of the management of your digital continuity, such as data quality.

5.4 DROID – our free file characterisation tool

The National Archives' file identification tool DROID can help you to understand your digital information better – for example, how much there is, how old it is, and what formats it comes in. The tool is available to download from The National Archives' website.

5.5 More information

If you would like more information on any of the matters arising from this, or any other guidance, please contact the Information Management team.

Appendix: Case studies

If you want to know what can happen if you don't manage your digital continuity, read these case studies. Each demonstrates what can happen if you can't find, open, work with, understand and trust your information.

You can't find the information you need: Atlantic hurricane case study

The arrival of Hurricanes Rita and Katrina in 2005 came during a state-wide IT upgrade. The city of Houston had begun to upgrade their outdated systems for procurement, asset management and payroll to integrate its financial-accounting systems with other functions.

When the hurricanes struck Houston, the city authority had to spend a large amount of time and manpower accessing disaster preparation data from their outdated asset management system, which it was required to do to meet federal emergency-assistance requirements. The asset management upgrade and financial accounting system integration would have enabled the city to deal with post-hurricane management situation, but these were not yet fully implemented. As it was, this caused disruption in the effort to get refugees back to Houston after they were displaced by the hurricanes.

You can't open the information you need: The Ivar Aasen Centre case study

The Ivar Aasen Centre in Norway is the national centre for Norwegian written culture and is devoted to the work of Ivar Aasen, 19th century scholar of Norwegian language and dialects.

In 2002 the centre found itself unable to access a catalogue holding information on around 11,000 literary works, which had taken the centre four years to create. The catalogue was stored in an encrypted database format, and only the two people who had donated and catalogued the collection, knew the sequential passwords required for access. Unfortunately, both men had died and no one at the centre knew the passwords.

A librarian at the centre attempted to access the database without success, so the centre issued an open invitation (with a reward attached) to IT experts worldwide to attempt to crack the code. Eventually the code was cracked by a Swedish computer programmer.

You can't work with the information in a way that you need to: *Toy Story* case study

When Pixar began creating animations for *Toy Story 3*, the team went back to take a look at their work on the original film (*Toy Story* 1995) and found they couldn't use the files.

Director Lee Unkrich says that the team were unable to open graphic files from the original film. Unkrich said, 'It's like a read-only file. Ultimately, we could look at the images but we couldn't do anything with them'. In the 15 years since the first film, it is likely that changes in technology meant they could no longer use the information in the way they needed to.

You can't understand your information: LeCrossing case study

The LeCrossing Company – responsible for the Dartford Crossing traffic management systems – used a system known as eCabinet document imaging to store and retrieve information in a wide variety of file types. When the company changed ownership it became apparent that the system was no longer supported by its manufacturer and had become obsolete, with the data locked inside. The information was inaccessible.

The context of the information had also been lost – image files (scanned files) and metadata had become separated, so documents could not be opened and understood.

LeCrossing's new owners Connect Plus also wanted to do more with the information than just view it. They wanted to export the data onto their own document imaging system and make it usable.

LeCrossing had to consult another company to attempt to solve these problems. It converted, extracted and captured the files and metadata from the eCabinet system. The files could then eventually be imported into a new data repository so they could be opened, viewed and understood.

You can't trust information is what it says it is: Japan pensions case study

In 2007, the Japanese government faced a crisis sparked by poor record-keeping in the Social Insurance Agency. One factor contributing to the problem was the introduction in 1997 of a new system to integrate multiple pension numbers into one single number for each person. However, the records were not properly maintained and handled, and by 2007, 50 million pension records couldn't be linked to the individuals who had been making payments.

The Parliamentary session due to end in July 2007 had to be extended to rush through laws to reform the department involved, a bill to abolish the statute of limitations on pensions, and a further bill to reform the civil service.

The government was faced with matching the 50 million unattributed pension records against the payment records of 100 million people – the entire population of those paying into the pension system, or receiving

payments. It has also guaranteed that everyone who made pension contributions will receive the pensions due to them.

In January 2008, the new Prime Minister announced, 'The careless management of public documents, such as pension records, is absolutely unacceptable. We will conduct a fundamental review for managing administrative records and will consider their legislation, and furthermore, we will improve the system for preserving public records, including expanding the national archives.' Japan's pension system is still recovering from this incident.